CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6212.01C
DISTRIBUTION: A, B, C, J 20 November 2003

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure O

1. Purpose. This instruction

a. Establishes policies and procedures for the J-6 interoperability requirements and supportability certification and validation of Joint Capabilities Integration and Development Systems (JCIDS) Acquisition Category (ACAT) programs cited in references a and b, and for all non-ACAT and fielded systems.

b. Provides detailed instructions for the implementation of information technology (IT) and National Security Systems (NSS) interoperability and supportability certifications as referenced in CJCSI 3170.01 Series, DODD 4630.5, DODI 4630.8, and DODD 8100.1 (references a, b, e, g and y, respectively).

c. Details the Net-Ready Key Performance Parameter (NR-KPP) in lieu of the Interoperability KPP (I KPP) discussed in CJCSI 3170.01C and CJCSM 3170.01. The NR-KPP shall be used to assess information needs, information timeliness, information assurance, joint interoperability and supportability, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP shall consist of measurable, testable or calculable characteristics and performance metrics required for the timely, accurate and complete exchange and use of information.

d. Establishes policies and procedures for Joint Interoperability Test Command (JITC) system interoperability test certification.

e. Provides additional guidance for development of Information Support Plans (ISPs) and establishes procedures for certification of ISPs

for all programs, including ACAT, non-ACAT, and fielded systems with regard to the J-6 interoperability requirements and supportability certification. The ISP replaces the Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP) originally in the DOD 5000 series directives.

2. Cancellation. CJCSI 6212.01B, 8 May 2000, Interoperability and Supportability of National Security Systems, and Information Technology Systems is canceled.

3. Applicability

a. This instruction implements the policies and procedures for developing, evaluating and providing interoperability and supportability certification in support of the JCIDS, which replaces the Requirements Generation System for ACAT, non-ACAT and fielded capabilities. This instruction applies to Services, combatant commands, Joint Staff, Defense agencies, and joint and combined activities. This instruction also applies to other agencies preparing and submitting JCIDS documents in accordance with references d and e.

b. This instruction is applicable to all IT and NSS (systems or services) acquired, procured or operated by any component of the Department of Defense, to include:

(1) All ACAT programs, non-ACAT activities and procurements, and fielded systems. ACAT programs include all DOD 5000-Series IT and NSS acquisition systems. Non-ACAT activities and procurements include all defense technology IT and NSS projects, IT and NSS pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations (ACTD), Advanced Technology Demonstrations (ATD), and Joint Warrior Interoperability Demonstrations (JWID) when selected for acquisition or procurement), joint experimentations, Joint Tests and Evaluations (JTE); non-DOD 5000 Series IT and NSS acquisitions or procurements (e.g., the Combatant Commander Command and Control Initiative Program (C2IP), Combatant Commander Initiatives Fund (CCIF), Combatant Commander Field Assessments, military exploitation of reconnaissance and technology programs, and tactical exploitation of national capabilities programs). Fielded systems are post-acquisition IT and NSS operational systems.

(2) All inter- and intra- component IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, coalition, and interagency operations and simulations.

(3) All IT and NSS acquired, procured, or operated by DOD intelligence agencies, DOD component intelligence elements, and other DOD intelligence activities engaged in direct support of DOD missions. This instruction recognizes that special measures may be required for protection and/or handling of foreign intelligence or counterintelligence information, or other need to know information. Accordingly, implementation of this instruction must be tailored to comply with separate and coordinated Director of Central Intelligence (DCI) directives and intelligence community policies.

(4) All DOD IT and NSS external information exchange interfaces with other US government departments and agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization).

c. The overall objective of this policy decision is to develop, acquire, and deploy IT and NSS that (1) meet the essential operational needs of US forces; (2) are interoperable with existing and proposed IT and NSS; (3) are supportable over the existing and planned global information grid; and (4) are interoperable with allies and coalition partners.

d. This instruction applies to any organization that supports the Joint Requirements Oversight Council (JROC) in its role to advise the Chairman of joint interoperability between existing and future IT and NSS.

e. All classified programs will comply with this instruction, but processes will be tailored to account for special security considerations.

f. This instruction does not preclude the need to refer to basic guidance and direction on defense acquisition and interoperability (references a through e and g).

4. Scope

a. This instruction addresses the interoperability and supportability of IT and NSS. This policy applies to all ACAT, Non-ACAT and fielded programs. IT and NSS are defined in Part II of the Glossary. Intelligence supportability is addressed in a separate, but related, process conducted by the J-2. Information assurance (IA) accreditation is addressed through the references d, f and r through w; IA accreditation for sensitive compartmented information (SCI) systems is addressed in references z, aa and bb.

b. This document removes most references to automated information systems (AIS) as defined in Part II of the Glossary. The generation and

implementation of AIS requirements involve unique circumstances and the user is directed to use the basic process in reference d. When modifications are absolutely essential to accommodate the unique aspects of a particular capability or system, they will be accomplished with approval of the Validation Authority.

5. Policy

a. It is DOD policy that all IT and NSS and major modifications to existing IT and NSS will be compliant with the Clinger-Cohen Act, DOD interoperability regulations and policies, and the most current version of the DOD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DOD system is a continuous process that must be managed throughout the lifecycle of the system. The NR-KPP is comprised of the following elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), applicable Global Information Grid (GIG) Key Interface Profiles (KIP), DOD information assurance requirements, and supporting integrated architecture products required to assess information exchange and use for a given capability.

b. This document explains the processes necessary to implement full-spectrum interoperability from an integrated and net-centric approach. To accomplish this, consideration will be placed on information needs, information timeliness, information assurance and net-enabled concepts using integrated architectures for a given capability. The NR-KPP is a mandatory element of all JCIDS documents and is required to receive interoperability certification.

c. Formats and processes in this instruction are mandatory for all ACAT, non-ACAT and other fielded capabilities. In most cases, this document will refer to references a and b for formats of capability documents. This document will provide additional information as it applies to supportability certification.

d. The J-6 certification process is an integral part of the JCIDS process. Interoperability requirements certifications granted under the former requirements generation system remain valid except as detailed below:

(1) The I-KPP contained in capstone requirements documents (CRDs) and Operational Requirements Documents (ORDs), already approved or directed by the JROC prior to JCIDS implementation, will continue to be valid until superseded by completed integrated architectures. The new JCIDS supports new CRDs directed by the JROC. Those new CRDs will develop their NR-KPP in accordance with

(IAW) the procedures documented in Enclosure D. The I-KPP currently cited in CJCSI 3170.01C and CJCSM 3170.01 has been superseded by the NR-KPP and meets the intent of JROC direction.

(2) Mission Needs Statement (MNSs) that have initiated staffing in the Joint C4I Program Assessment Tool will continue through the normal staffing process; however, J-6 will assess MNS but will not certify for interoperability requirements certification. J-6 will only concur or nonconcur based upon interoperability concerns and implications. IAW references a and b, no new MNS will be accepted for staffing.

(3) IAW references a and b, ORDs will be accepted for staffing IAW the current CJCSI 3170.01B, dated 15 April 2001, for 6 months after signing CJCSI 3170.01C, i.e., until 24 December 2003, unless otherwise extended by the JROC. Therefore, I KPP for those documents will be IAW CJCSM 3170.01M Enclosures B and H. Enclosure H will be superseded automatically upon the termination of ORDs on 24 December 2003.

(4) All JCIDS documents submitted for review and interoperability certification will be submitted into the J-8 Knowledge Management/Decision Support (KM/DS) tool. Users should contact the J-8 at 703-695-7065 for details.

(5) All ISPs for all ACAT programs will be submitted into the OSD Joint C4I Program Assessment Tool (JCPAT) tool for review on the SIPRNET at https://206.36.228.76.

e. Unless declared unsuitable for information sharing due to national security considerations, for purposes of interoperability and supportability, all IT and NSS developed for use by US forces are for joint, combined, and coalition use. The term “joint force” throughout this document refers to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander (JP 1-02 and references e and g). Interoperability and supportability of IT and NSS requirements for ACAT programs will be determined during the JCIDS validation process (references a through e and g) and this instruction and will be updated as necessary throughout the acquisition period, deployment and operational life of a system. Interoperability and supportability of IT and NSS requirements for non-ACAT and fielded programs will be determined by the requirements authority IAW references c, d, e and g and this instruction and will be updated as necessary throughout the acquisition period, deployment, and operational life of a system.

6. Implementation and Supplementation. Upon implementation of this instruction, the interoperability and supportability certification process for all IT and NSS (classified SECRET and below) will use the J-8 Knowledge Management/Decision Support (KM/DS) tool for JCIDS document staffing and the Joint C4I Program Assessment Tool (JCPAT) for Information Support Plan staffing. Documents established in staffing at the time of implementation of this instruction will convert to KM/DS at the next key-staffing milestone. The Web site for KM/DS is https://siprweb1.js.smil.mil/pls/jrcz. JCPAT is the integrated tool used by J-6 and DISA for managing the interoperability and supportability certification, testing, and validation process end-to-end and involves system and/or program registration, standards development, capability interconnectivity, and interoperability analysis, testing, certification, and validation. This instruction will not be supplemented without the prior approval of the Vice Chairman of the Joint Chiefs of Staff or his delegated representative.

7. Waivers. Submit waivers or requests for exceptions to the provisions of this instruction to the Joint Staff. Statutory requirements shall only be waived if the statute specifically provides for doing so. All JCIDS documents and ISPs submitted 6 months after publication of this instruction shall contain the NR-KPP defined in this instruction. Legacy Requirements Generation System (RGS) documents and CRDs will continue to contain the legacy I KPP. When the NR-KPP requirement is waived, an alternate J-6 approved source of interoperability requirements information will be specified by J-6.

8. Summary of Changes

a. This revision reflects a complete rewrite of the document to reflect changes in the overall acquisition and new capability based methodology. The revision also reflects a new NR-KPP and other changes that support an integrated view of architectures.

b. This revision reflects recent changes from the DOD 5000-series, DODD 4630.5, DODI 4630.8, and CJCSI 3170 (references a, c, d, e and g).

9. Releasability. This instruction is approved for public release and distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page – http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Electronic Library CD-ROM.

10. Definitions. See Glossary.

11. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

T. J. KEATING
VADM, USN
DIRECTOR, JOINT STAFF

Enclosures:
A--Process Overview
B--Responsibilities
C--Procedures
D--Capstone Requirements Document (CRD)
E--Initial Capabilities Document (ICD)
F--Net-Ready Key Performance Parameter for the Capability Development Document (CDD)
G--Net-Ready Key Performance Parameter for the Capability Production Document (CPD)
H--Requirements Generation System Documents
I--Information Support Plan (ISP)
J--Joint C4I Program Assessment Tool – Empowered (JCPAT-E)
K--Interconnectivity and Interoperability Capability (IIC) Profile
L--IT Standards Profile
M--Joint Interoperability Testing and Test Certification Process
N--IT and NSS System Specific Policies
O--References
GL--Glossary

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 8	O	H-A-1 thru H-A-6	O
i thru viii	O	I-1 thru I- 18	O
A-1 thru A-22	O	I-A-1 thru I-A-6	O
B-1 thru B-14	O	J-1 thru J-8	O
C-1 thru C-8	O	K-1 thru K-2	O
D-1 thru D-10	O	L-1 thru L-6	O
E-1 thru E-12	O	M-1 thru M-8	O
F-1 thru F-16	O	N-1 thru N-2	O
G-1 thru G- 16	O	O-1 thru O-4	O
H-1 thru H- 4	O	GL-1 thru GL-14	O

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

PROCESS OVERVIEW

1. This enclosure provides an overview of the J-6 Interoperability and Supportability Certification and Interoperability Certification Testing Process. Detailed procedures are provided in Enclosure C.

2. Failure to meet Certifications

a. If a program/system fails to meet certification requirements, the J-6 will:

(1) Not validate the program.

(2) Recommend the program not proceed to the next milestone.

(3) Recommend that funding be withheld until compliance is achieved and the program and/or system is validated.

b. The J-6 will make this recommendation to the USD(AT&L), USDP, USD(C), ASD(NII), DOD Executive Agent for Space, the Military Communications-Electronics Board (MCEB), and the JROC. The J-6 will also request that the program and/or system be added to the DODI 4630.8, Interoperability Watch List (IWL).

3. Net-Ready Key Performance Parameter (NR-KPP)

a. The focus of the new interoperability and supportability certification process is the NR-KPP, which replaced the previous I KPP.

b. The NR-KPP assesses net-readiness; information assurance requirements; and both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of measurable and testable characteristics and/or performance metrics required for the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP, documented in CRDs, Capabilities Development Document (CDD)s and Capabilities Production Document (CPD)s, shall be used in analyzing, identifying and describing IT and NSS interoperability, and test strategies in the Test and Evaluation Master Plan (TEMP).

c. The NR-KPP consists of the following elements:

(1) Information Assurance. Demonstrate achievement of Information Assurance within the GIG through a defense-in-depth approach that integrates the capabilities of personnel, operations and technology, and supports the evolution to network centric operations and warfare. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD IT and NSS systems in accordance with 10 USC Section 2242, OMB Circular A-130 Appendix III, and references r through w; as well as references z, aa and bb for SCI and Special Access Programs. Interoperability and integration of IA solutions within or supporting the DOD shall be achieved through adherence to an architecture that will enable evolution to network centric operations and warfare by remaining consistent with the DOD Architecture Framework, and defense-in-depth approach.

(2) Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW RM). The NCOW RM, depicted in Figure A-1, describes the activities required to establish, use, operate and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (COI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG are realized. The NCOW RM represents the objective end-state for the GIG. (See reference n for details.) This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations.

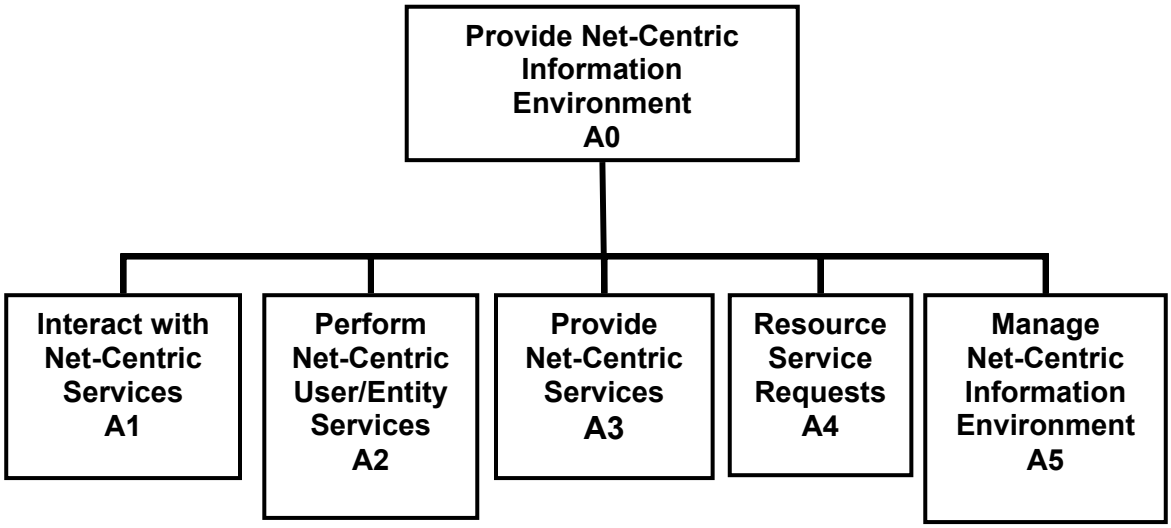

Figure A-1. Net Centric Operations Warfare Reference Model (NCOW RM)

(a) The NCOW RM serves as a common, enterprise-level, reference model for the DOD's Enterprise Architecture and for current and future acquisition programs to use in focusing and gaining net-centric support through the GIG. The NCOW RM enables a shared perspective of the enterprise information environment operations and is used to assist decision-makers in arriving at decisions that promote enterprise-wide unity of effort. The goal is to perform program development and oversight with a uniform Department-wide reference to which all net-centric IT-related issues can be addressed within individual programs and across the set of enterprise programs in a constructively consistent, coherent, and comprehensive manner. The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities core services, community of interest (COI) services, and environment control services, and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the GIG become realized.

(b) The NCOW RM represents the target viewpoint of the DOD GIG. This viewpoint is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of (1) military operations, (2)

DOD business operations, and (3) Department-wide enterprise management operations. Enterprise management operations extend from internally focused operations to externally focused operations in which the DOD is one component of the total US government enterprise. The NCOW RM will ultimately provide a common architectural construct for NCOW with a common language and taxonomy. The final version of the RM will include:

1. All Views (AV): AV-1 and AV-2

2. Operational Views (OV): OV-1, OV-2, OV-3, and OV-5

3. System Views (SV): SV-1, SV-2, SV-3, SV-4, and SV-5

4. Target Technical View

(c) The current version, NCOW RM v0.9, consists of the following architectural view products:

1. All Views: AV-1, AV-2

2. Operational Views: OV-1, OV-5

3. Target Technical View

(1) Compliance with applicable GIG Key Interface Profiles (KIPs). GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. (See reference n for details.)

(a) A KIP is the set of documentation produced as a result of interface analysis which:

1. Designates an interface as key.

2. Analyzes it to understand its architectural, interoperability, test requirements, configuration management and security requirements.

3. Documents those characteristics in conjunction with solution sets for issues identified during the analysis.

(b) The profile consists of:

1. Refined operational and systems view products.

2. Interface Control Document/Specifications.

3. Engineering Management Plan.

4. Configuration Management Plan.

5. Technical Standards View (TV-1) with SV-TV Bridge.

6. Procedures for standards conformance and interoperability testing.

(a) DOD identified 17 key interfaces in reference cc for development and management at the enterprise level. DISA developed the GIG teleport KIP in November 2002.

(b) Relevant GIG KIPs, for a given capability, shall be documented in the CDD and CPD. Compliance with identified GIG KIPs shall be analyzed during the development of the ISP and TEMP, and assessed during DISA (JITC) joint interoperability certification testing. Since all of the GIG KIPs have not been developed, the following applies:

(c) The Chairman of the Joint Chiefs of Staff and DISA shall continue the development of the GIG KIPs.

(d) The Chairman of the Joint Chiefs of Staff shall continue the well-defined, phased implementation of the GIG KIPs, to be completed by FY 2006.

(e) DISA shall maintain completed GIG KIPs in the DOD DISR), an online database registry for standards and profiles.

(2) Supporting Integrated Architecture Products. The following integrated architecture products described in reference e shall, as a minimum, be incorporated in the NR-KPP and used to assess information exchange and use for a given capability:

Framework Products	Framework Product Name	General Description
AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
OV-2	Operational Node Connectivity Description	Operational Nodes, operational activities performed at each node, connectivity and information exchange need lines between nodes
OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
OV-5	Operational Activity Model	Operational activities, relationships among activities, inputs and outputs. Overlays can show cost performing nodes, or other pertinent information.
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity sequence and timing – traces actions in a scenario or sequence of events and specifies

		timing of events.
SV-4	Systems Functionality Description	Functions performed by systems and the information flow among system functions, including information assurance functions
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to operational capabilities or of system functions back to operational activities.
SV-6	Systems Data Exchange Matrix	Provides details of systems data being exchanged between systems.
TV-1	Technical Standards Profile	Extraction of standards that apply to the given architecture, Including information assurance functions.

Table A-1. Principal Integrated Architecture Products.

a. The NR-KPP for each type of document (CRD, CDD, CPD and ISP) is defined in the applicable enclosure in this document. Table A-2 provides a matrix of the JCIDS documents and the NR-KPP architecture products. As indicated above, at a minimum, the NR-KPP is comprised of:

(1) Supporting Architecture products.

(2) Compliance with the NCOW reference model.

(3) Compliance with the KIP.

(4) Information Assurance policies and procedures.

Document	Net-Ready Key Performance Parameter Products																	LISI Profile
	Supporting Architecture Products														NCOW RM	KIP Compliance	IA Compliance	
	AV-1	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	SV-1	SV-2	SV-3	SV-4	SV-5	SV-6	TV-1				
ICD		X													X			
CDD	X		X		X	X	X				X	X	X	X	X	X	X	X Basic
CPD	X		X		X	X	X				X	X	X	X	X	X	X	X Complete
CRD		X		1		2									2	2	2	
ISP	3	3	3		3	3	3	3			3	3	3	3	3	3	3	3 Complete

Note: X = Required
(1) Old CRDs Updates
(2) New CRDs
(3) ACAT, NON ACAT and Fielded Systems. NR-KPP products produced for the CDD and CPD will be used in the ISP.

Table A-2. JCIDS Documents/NR-KPP Products Matrix.

b. All elements of the NR-KPP will be able to be measured, tested or evaluated.

4. Migration to the Net-Ready Key Performance Parameter. Just as was done with CJCSI 3170 regarding top down architectures, it is recognized that all the KIPs are not available, but the process must be put in motion for future system development.

a. Figure A-2 below depicts the migration timeline to the NR – KPP.

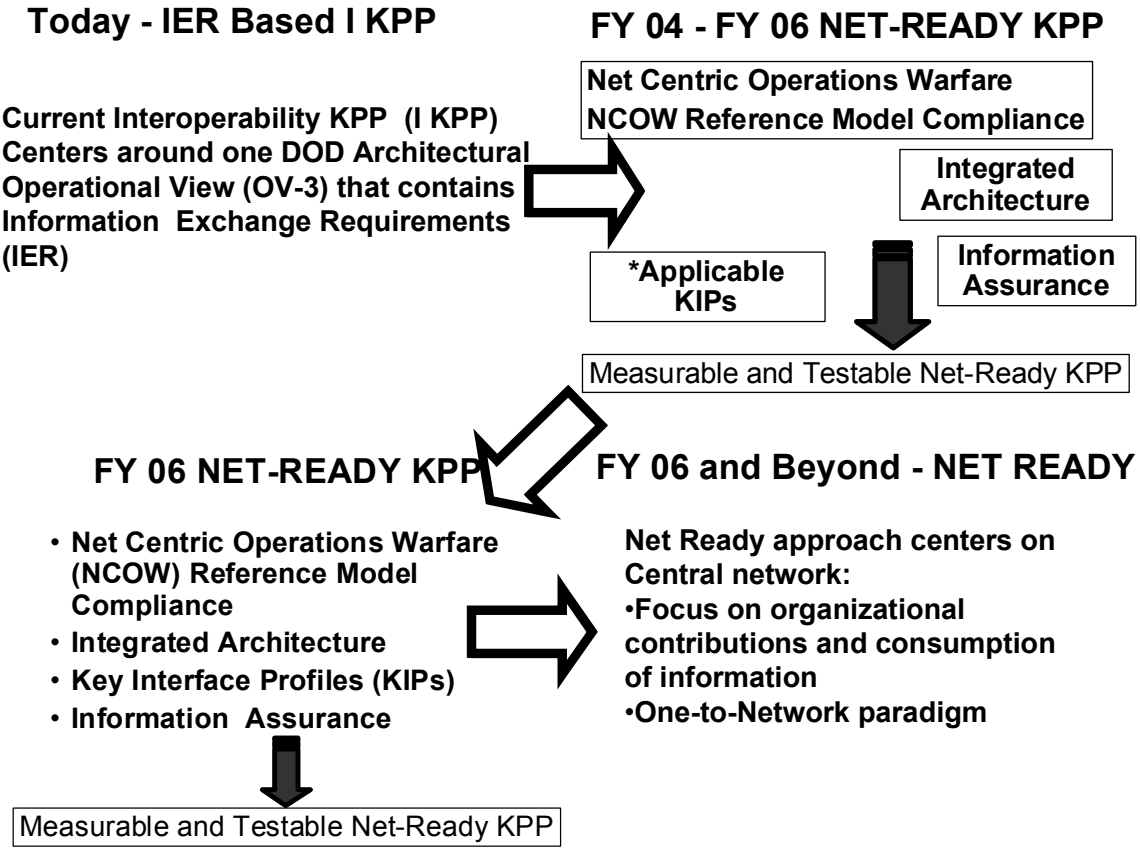

Figure A-2. Migration to the Net-Ready KPP

b. FY 04 to FY 06. Program managers will comply with three parts of the Net-Ready Key Performance Parameter:

(1) Architectures products. See Table A-2. Program Managers (PM) producing the Architectures Products, using the NCOW RM, should develop high-level interface information for becoming net ready and plan to be Key Interface compliant to the applicable KIPs as they become available.

(2) Net-Centric Operations Warfare Reference Model. NCOW RM provides the PM with a common lexicon for NCOW concepts and

terminology, supported by recognizable architectural descriptions. It describes net-centricity at the enterprise level for DOD Program Managers and other decision makers. It includes Overview And Summary Information (AV-1), Integrated Dictionary (AV-2), High-Level Operational Concept Graphic (OV-1), Activity Model (OV-5), and Target Technical View (TV-1).

(3) Information assurance. IAW DOD Directive 5000.1 (reference d, PMs shall verify compliance with the security requirements and evaluate vulnerabilities, for each lifecycle development activity where there is a corresponding set of security activities. PMs must provide J-6 documentation that each phase of the Defense Information Technology Security Certification and Accreditation Program (DITSCAP) process (Definition, Verification, and Validation) has been completed throughout the stages of the JCIDS/acquisition process.

(4) As key interfaces which have been profiled and made available through the DISR, PMs will comply with these KIPs, which will be published as an annex in DISR. KIP's will be distributed as an advisory as soon as they have been defined, and will be formally published on a priority basis. PM's are required to incorporate published KIP's in all new start or significantly modified systems acquisitions and/or pre-Milestone B designs immediately. For ongoing acquisitions beyond Milestone B and/or established systems, published KIPs will be included as objective capabilities immediately, and as threshold requirements within 12 months of publication through the systems evolutionary spiral block upgrade process.

c. FY 06 and beyond. PMs will be expected to comply with all parts of the NR-KPP.

5. This instruction must account for three categories of programs requiring certification: ACAT programs which enter into the JCIDS process (references a and b), Non-ACAT programs, and fielded systems. The following paragraphs provide an overview of the processes for conducting interoperability and supportability certification and testing certification for these three categories.

a. ACAT Programs. This paragraph provides policy for interoperability and supportability certification and for Joint System Interoperability Test Certification of ACAT programs.

(1) Interoperability and Supportability Certification and Validation Process for ACAT Programs. Figure A-1 depicts the interoperability and supportability certification process for ACAT

programs. This diagram illustrates three interoperability and two supportability certifications of capabilities and one validation of the completed systems tests against required capabilities and architectures discussed in the following paragraphs. The J-6 will certify capabilities interoperability and supportability for all IT and NSS for all ACAT.

(a) The J-6 interoperability and supportability certification and testing validation process is intended to manage, evaluate, and report IT and NSS interoperability and supportability over the life of the system.

(b) The J-6 will validate that the following have been accomplished: capabilities interoperability and supportability certification; JITC Joint System Interoperability Test Certification; and NR-KPP: NCOW Reference Model compliance, integrated architecture products compliance, KIPs compliance; and information assurance accreditation.

(2) The interoperability and supportability certification process for all IT and NSS (classified SECRET and below) will use the J-8 KM/DS tool for JCIDS document staffing and the JCPAT for ISP staffing. JCPAT is the integrated tool used by J-6 and DISA for managing the interoperability and supportability certification, testing, and validation process end-to-end and involves system and/or program registration, standards development, capability interconnectivity, and interoperability analysis, testing, certification, and validation. Figure A-3 depicts the interoperability and supportability certification, testing and validation process for ACAT programs.

(a) Developmental (CDD) interoperability requirements and supportability certification occurs prior to acquisition Milestone B. For space systems being acquired under reference dd, the CDD is required prior to PDR.

(b) Production (CPD) interoperability requirements certification and supportability certification occurs prior to acquisition Milestone C.

(c) PMs will submit JCIDS documents for interoperability certification into the J-8 KM/DS tool. PMs will submit ISPs for all ACAT, Non-ACAT and fielded systems for supportability certification into the OSD JCPAT tool for review. The ISP is submitted prior to key decision point (KDP-B) and update is submitted prior to KDP-C for space systems acquired under reference dd.

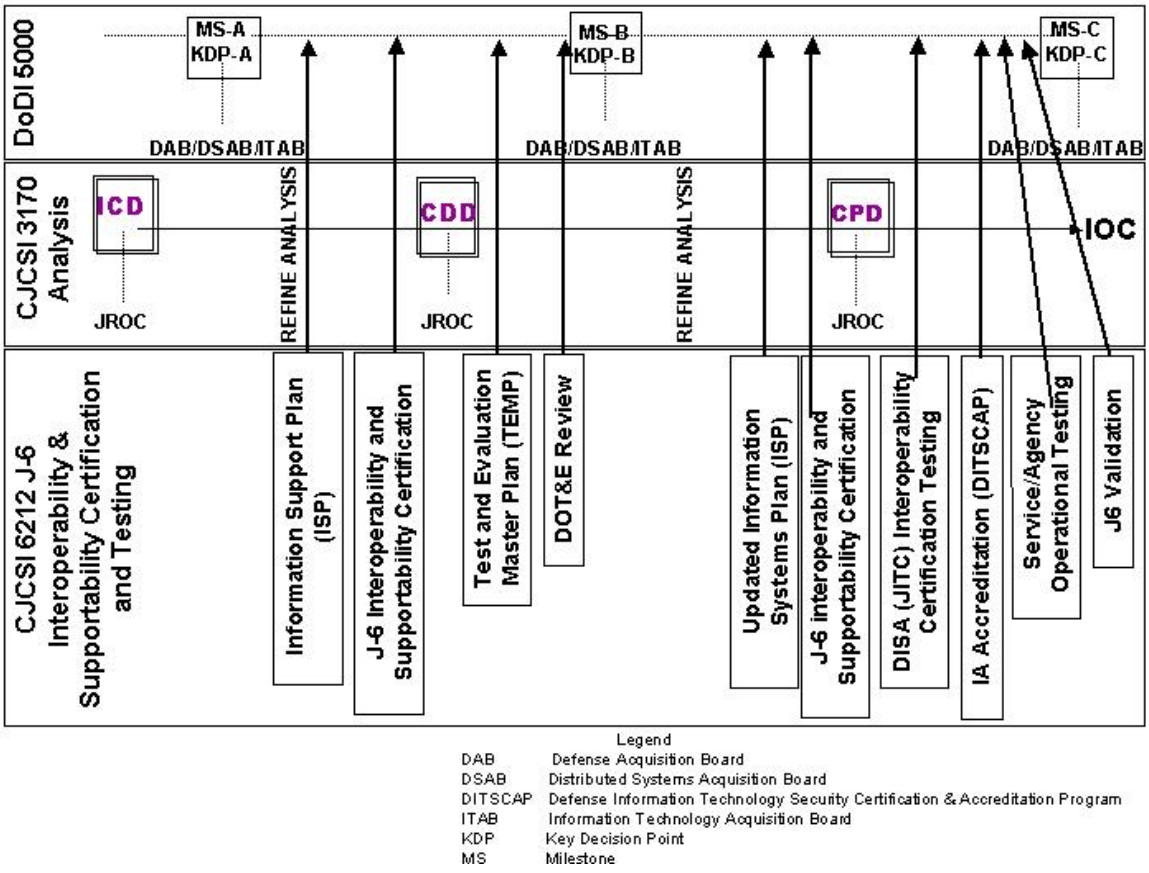

Figure A-3. J-6 Interoperability and Supportability Certification, Testing, and Validation Process for ACAT Programs

(d) During the review process, J-8 staffs JCIDS documents on KM/DS to OSD, combatant commands, Services, the Joint Staff and DOD agencies.

(e) ASD(NII) staffs ACAT I and OSD Special Interest ISPs and J-6 staffs all other ACAT ISPs on JCPAT to OSD, combatant commands, Services and DOD agencies.

(f) Only the J-6 will certify interoperability and supportability requirements for JCIDS documents and ISPs for all ACAT, to ensure conformance with policy, doctrine, and applicable interoperability and supportability standards for joint IT and NSS. J-6 reviews all interoperability and supportability related comments submitted into KM/DS and JCPAT as part of the certification process. All interoperability comments submitted to the KM/DS tool will be identified in the KM/DS Comment Matrix by inserting “Interoperability Comment”

as the first entry in the COMMENT column. Only comments so marked will be considered as part of the interoperability certification process.

(g) Combatant commanders are asked to review and provide comments on all ACAT programs during the interoperability and supportability certification process.

(h) US Joint Forces Command (USJFCOM), as the joint force integrator, will review and confirm sufficiency of NR-KPPs and integrated architectures for JCIDS documents regardless of ACAT. USJFCOM, as the Chairman's advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the Joint C4ISR battle center's (JBC) interoperability technology demonstration center (ITDC). Selection of the program or system may be made by the joint battle management command and control board of directors. These interoperability demonstrations do not replace the JITC system interoperability test certification. Demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

(i) After completing the two-stage document review, sponsors will submit the adjudicated comment resolution matrix and updated ORD/ICD/CDD/CPD to J-8 KM/DS tool (for JCIDS documents) or adjudicated comments resolution matrix and updated ISP to JCPAT (for ISPs). Sponsors will upload these documents into KM/DS or JCPAT (respectively) and contact J-6 to request interoperability and/or supportability certification for all JCIDS and/or ISP documents not originally granted certification after the flag level and/or certification review.

(j) The J-6 will provide interoperability and supportability requirements certification for JCIDS documents (CRD, CDD, and CPD), regardless of ACAT level, designated as JROC Interest, Joint Impact, and Joint Integration. The J-6 will provide supportability certification for ISPs for all ACAT regardless of ACAT level. All inter- and intra-DOD component IT and NSS that exchange and use information to enable units or forces to operate effectively in joint, combined, and interagency operations shall be certified for interoperability and supportability. Programs categorized as independent (e.g., systems or capabilities that do not exchange or use external information) are returned to the submitter and do not require certification.

(k) In accordance with reference g, the PM for all ACAT programs will submit an ISP into the DOD JCPAT tool for review prior to Milestone B (Program initiation for ships) and an updated ISP prior to

Milestone C in accordance with DOD 5000.2-R or Acquisition Deskbook (as appropriate) guidance. The ISP shall describe system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance, and interoperability issues. Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO) will coordinate the review of ACAT I and Special Interest ISPs. The J-6 will coordinate the review of ACAT II and below (non-Special Interest) ISPs.

(l) The J-6 provides supportability certification to ASD(NII)/DOD CIO and posts this certification onto JCPAT and KM/DS for all CPDs including all ACAT programs, regardless of ACAT level. This certification ensures that IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, and identify dependencies and interface requirements between systems are adequately addressed. This is done prior to Milestone C.

(m) In support of a Milestone C decision, J-6 will provide validation of status of interoperability and supportability requirements certification (JITC Joint System Interoperability Test Certification), adherence to the NCOW Reference Model, information assurance accreditation, and achievement of the NR-KPP, to the Milestone Decision Authority (MDA).

(n) In support of the J-6 JCIDS document certification, DISA JITC will review and confirm the measurability and testability of all NR-KPPs.

(3) <u>IT and NSS Joint System Interoperability Test Certification for ACAT Programs</u>.

(a) All ACAT IT and NSS must be evaluated and certified for Joint interoperability by DISA (JITC). When JITC is not the responsible testing organization, the system proponent will coordinate test plans, analysis, and reports with JITC to ensure sufficient information is available to support a certification determination. IT and NSS interoperability testing and evaluation shall be conducted as early as is practical to support scheduled acquisition or procurement decisions during the development phases and throughout a system's life. Testing may be performed in conjunction with other testing (i.e., Developmental Test & Evaluation (DT&E), Operational Test and Evaluation (OT&E), or

early user test) whenever possible to conserve resources. Enclosure M describes the Joint System Interoperability Test Certification process.

(b) All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint System Interoperability Test Certification (see reference g). J-6 may waive the requirement for an NR-KPP on a case-by-case basis. (When waived, the source of interoperability requirements needs to be satisfied.)

(c) The table below provides the NR-KPP Threshold and Objective:

Net-Ready KPP	**Threshold (T)**	**Objective (O)**
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture**.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture.

Table A-3. NR-KPP Threshold and Objective

* Data processing is defined as: the input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.
** Joint integrated architecture: An integrated architecture that establishes the basis for rapidly acquiring affordable and evolving joint warfighting capabilities through collaborative planning, analysis, assessment and decision making.

(d) The MDAs and component acquisition executives (CAEs) must address IT and NSS interoperability evaluation and certification by DISA (JITC) as an integral part of the acquisition process prior to production and fielding approval of each increment.

(e) DISA (JITC) Joint System Interoperability Test Certification evaluation will include standards conformance evaluation and certification, where applicable. DISA (JITC), in conjunction with the PMs, will plan and conduct standards conformance evaluation, including compliance with applicable Key Interface Profiles (KIPs), during the development and acquisition procurement processes. DISA (JITC) will provide input to the DT and Operational Test Readiness Review (OTRR) processes on whether a system is ready for testing, from an interoperability perspective.

(f) DISA (JITC) Joint Interoperability re-Certification is required as follows:

1. When materiel changes (e.g., hardware, firmware, software modifications) affect interoperability.

2. Upon revocation of interoperability certifications or J-6 system validation.

3. Upon automatic expiration 3 years after the date of the certification.

4. When non-materiel changes (i.e., Doctrine, Operations, Training, Logistics, Personnel, or Facilities) occur that may affect interoperability.

(g) IT and NSS with significant interoperability may be placed on the Interoperability Watch List (IWL) to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

b. Non-ACAT Programs. This paragraph provides policy for Interoperability and Supportability Certification and for DISA (JITC) Joint System Interoperability Test Certification of non-ACAT programs.

(1) This process applies to IT and NSS under consideration for operational use, but being acquired or procured outside of the ACAT program processes described in DOD 5000 Series (reference d). Included in this category are all defense technology projects and pre-acquisition demonstrations (e.g., Advanced Concept Technology Demonstrations

(ACTDs), Joint Testing and Evaluations (JT&Es), and Joint Warrior Interoperability Demonstrations (JWIDs) that lead to acquisitions), the Combatant Commander Command and Control Initiative Program, Combatant Commander Field Assessments, Military Exploitation of Reconnaissance and Technology Programs, Tactical Exploitation of National Capabilities Programs, DODIIS, post-acquisition (fielded) IT and NSS systems, and modifications to fielded IT and NSS capabilities.

(2) If the acquisition or procurement of non-ACAT IT or NSS or services transitions to an acquisition program, then it shall be managed and fielded per the DOD 5000 series guidance.

(3) Interoperability and Supportability Certification and Validation Process for Non-ACAT Programs

(a) Figure A-4 depicts the interoperability and supportability certification process and its linkage to the JCIDS process for Non-ACAT programs.

1. This diagram illustrates the Joint Staff interoperability and supportability review and certification of the ISP, JITC Joint Interoperability Test Certification, Information Assurance accreditation and a J-6 validation of the NR-KPP requirements for Non-ACAT programs (Certified ISP, IA Accreditation, and JITC Interoperability Certification).

2. The J-6 will certify interoperability and supportability capabilities for all Non-ACAT IT and NSS. The J-6 interoperability and certification and testing process is intended to manage, evaluate, and report IT and NSS interoperability and supportability over the life of the system.

3. The J-6 will validate that the following have been accomplished:

a. Interoperability and supportability requirements certification.

b. JITC Joint System Interoperability Test Certification. In support of the J-6 JCIDS documentation certification, DISA JITC will review and confirm the measurability and testability of all NR-KPPs.

c. Information assurance accreditation.

4. This interoperability and supportability certification process for all IT and NSS will use the Joint C4I Program Assessment Tool (JCPAT) and involves system/program registration, standards development, capability interconnectivity, and interoperability analysis and certification. Information assurance accreditation guidance is provided in reference u.

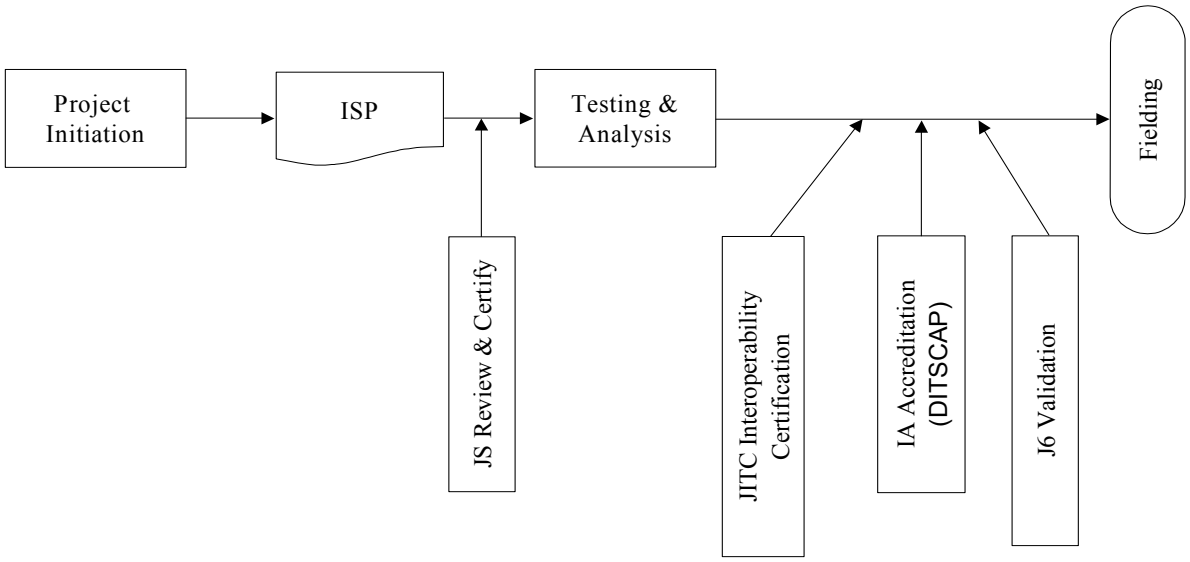

Figure A-4. Non-ACAT Interoperability and Supportability Certification Process

(b) Information Support Plan (ISP). In accordance with reference g, an ISP shall be developed for all non-ACAT acquisitions and procurements to document IT and NSS needs, dependencies, interface requirements and the NR-KPP. The plan shall describe system dependencies and interface requirements in sufficient detail to enable testing and verification of IT and NSS interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance, and interoperability issues. The scope of the ISP shall be scaled to the relative size and funding profile for the program. The sponsoring or cognizant authority shall review, assess, and approve the ISP for non-ACAT acquisitions and procurements, and

forward any critical interoperability or supportability issues to the ASD (NII)/DOD CIO.

(c) IT and NSS Joint Interoperability Certification Evaluation for Non-ACAT Programs. All non-ACAT acquisitions and procurements shall be tested and evaluated for required interoperability.

1. The fielding authority must address IT and NSS interoperability evaluation and certification during the system interoperability test certification by DISA (JITC) as an integral part of the requirements validation and acquisition process prior to procurement, production or fielding approval of each increment.

2. IT and NSS interoperability testing shall be scaled, as necessary, based on the relative size and funding profile, criticality, and other risk factors for the program and may be performed in conjunction with other tests, exercises or demonstrations (e.g., component interoperability testing) to conserve resources.

3. DISA (JITC) will conduct an interoperability evaluation, based on JITC system interoperability testing of the NR-KPP or other submitted test results, and provide a system interoperability test certification.

4. Other than the source of interoperability requirements, the operational interoperability evaluation and certification process remains the same as for ACAT systems. (Enclosure M describes the Joint System Interoperability Test Certification and evaluation process.)

5. The sponsoring or cognizant authority shall review and consider IT and NSS interoperability test results prior to operational use or fielding decision. IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), DPA&E, the ASD(NII)/DOD CIO, the DOT&E, DOD Executive Agent for Space, and the Chairman of the Joint Chiefs of Staff, and USJFCOM) may be placed on the IWL to ensure that sufficient attention is given toward achieving and maintaining interoperability objectives.

6. All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint Interoperability System Certification.

c. Fielded Systems. This paragraph provides policy for interoperability and supportability certification and for certification testing of fielded systems.

(1) Interoperability and Supportability Certification and Validation Process for Fielded Systems. The sponsoring authority will verify that all proposed materiel and non-materiel remedies for fielded IT and NSS capabilities meet interoperability and supportability requirements. IT and NSS interoperability verification may be performed in conjunction with other activities such as joint tests and evaluations, operational tests and exercises, demonstrations or component interoperability testing to conserve resources.

(a) A CPD/ISP must be submitted for fielded systems in order to receive an interoperability/supportability review and certification.

(b) Systems that cannot provide the required documentation must obtain an Interim Certificate to Operate (ICTO), issued by the MCEB interoperability test panel (good for up to 1 year), in order continue to operate until they provide the documentation.

(2) Figure A-5 depicts the interoperability process for addressing operational warfighting interoperability and supportability issues for fielded IT and NSS.

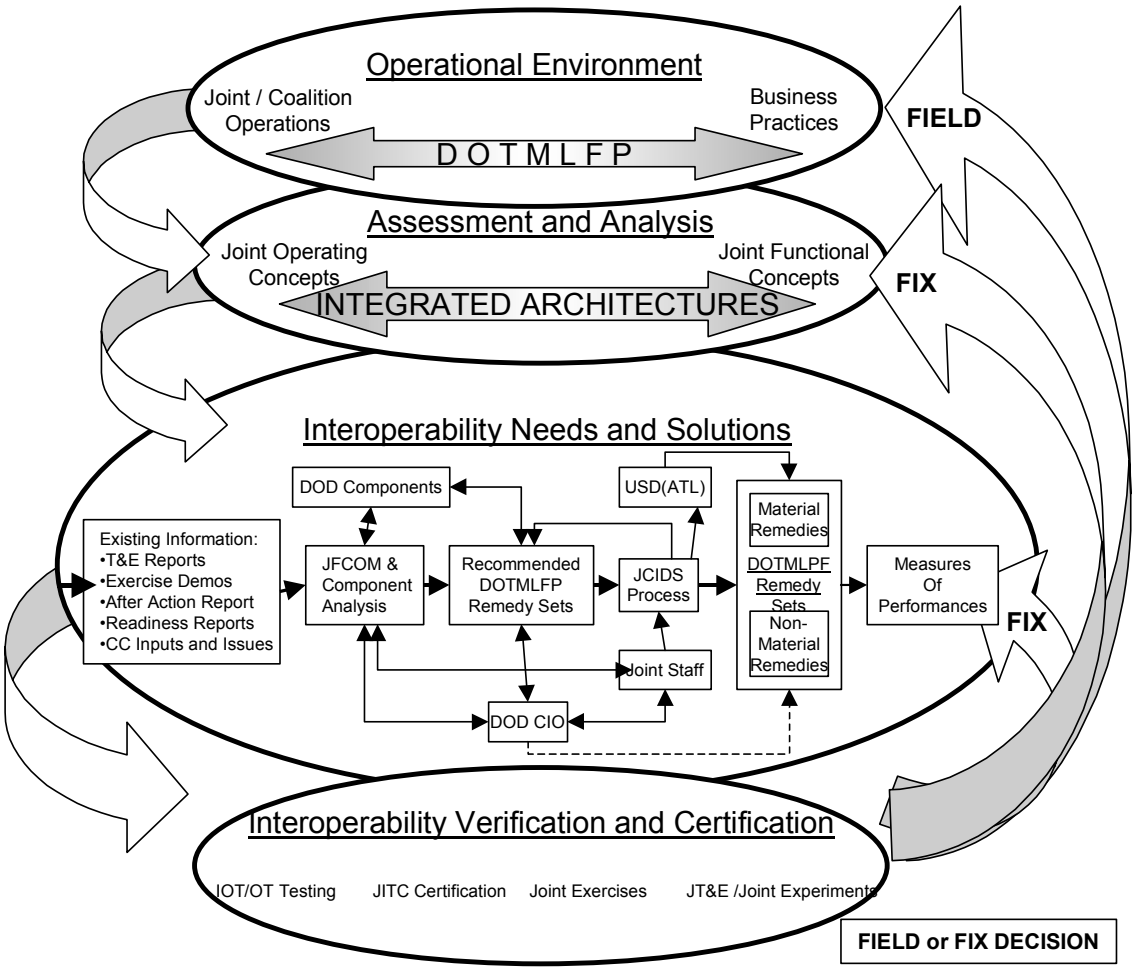

Figure A-5. Fielded (Legacy Systems) IT and NSS Interoperability Process

(3) IT and NSS Joint System Interoperability Test Certification for Fielded Systems. Other than the source of interoperability requirements,

the operational interoperability evaluation and certification process remains the same as for ACAT systems. (See Enclosure M for a description of the Joint Interoperability Certification test and evaluation process.)

(a) DISA (JITC) will conduct an interoperability evaluation, based on JITC system interoperability testing of the NR-KPP or other submitted test results, and provide a system interoperability test certification.

(b) The sponsoring authority for the materiel or non-materiel remedy shall review and consider IT and NSS interoperability test results prior to operational use or a fielding decision.

(c) IT and NSS with significant interoperability deficiencies (as determined by the offices of the USD(AT&L), the ASD(NII)/DOD CIO, the DOT&E, DPA&E, DOD Executive Agent for Space, the Chairman of the Joint Chiefs of Staff and the USJFCOM) may be placed on the IWL to ensure that sufficient attention is given towards achieving and maintaining interoperability objectives.

(d) All IT and NSS must have a J-6 certified NR-KPP prior to DISA (JITC) Joint Interoperability System Certification.

6. Interoperability Test Panel

a. The MCEB Interoperability Test Panel (ITP) resolves issues in joint testing and interoperability certification.

b. The ITP in special situations may, on a case-by-case basis, grant a temporary certification from interoperability system testing certification in the form of an Interim Certificate to Operate (ICTO).

c. Submit requests for an ICTO to the ITP IAW reference h (or see the DISA (JITC)/ITP Web site: http://jitc.fhu.disa.mil).

d. ICTOs will not exceed 1 year.

7. Joint System Interoperability Test Certification Programming and Budgeting

a. Combatant commands, Services and agencies are responsible for funding interoperability testing for systems. This responsibility includes funding, scheduling, and coordination to ensure that external interfacing systems are available during interoperability testing. Required

interoperability testing and certification will normally impact schedule and program cost and will need to be added to POM and program cost estimates.

b. Combatant commands/Services/agencies (C/S/A) may designate and fund another C/S/A test organization to conduct interoperability testing.

(1) When DISA (JITC) is not the interoperability testing organization, interoperability test plans, test analysis, and test reports will be coordinated with DISA (JITC) to ensure sufficient information is available to allow DISA (JITC) to certify a system.

(2) DISA (JITC) schedules tests and certifications, balancing between the program manager's schedule, DISA (JITC)'s available test resources, organizational priorities, and functional priorities. Enclosure M provides more information.

7. Joint System Interoperability Testing and Certification Prioritization. Combatant commands/Services/agencies and participating test unit coordinator (PTUC) will incorporate interoperability testing into its overall testing plans in coordination with DISA (JITC).

a. DISA (JITC) uses the following organizational prioritization for testing, assessing and certifying interoperability:

(1) Joint IT and NSS systems that support the unified commands.

(2) Joint IT and NSS systems that are acquired by the Services.

(3) Systems that are acquired by the Defense agencies.

b. The order for functional prioritization is:

(1) Strategic warning and communication systems that support the unified commands, the Secretary of Defense and the Commander-in-Chief;

(2) Tactical systems that support the unified commands;

(3) C2 systems that support the unified commands;

(4) Combat service support systems that support the unified commands.

c. Interoperability testing and certification schedule conflicts will be submitted to the ITP for resolution. Issues that cannot be resolved by the ITP process will be submitted to the MCEB for resolution.

d. The prioritization process is not intended to impede, delay, or restrict milestone accomplishment. Should delays occur due to a lack of testing resources, the PM should submit an ICTO request to the ITP.

8. Information Technology Standards. New or modified IT and NSS systems should be capabilities-based. IT and NSS must comply with applicable information technology standards contained in the current DISR, and the latest versions of the OASD(NII) Net Centric Operations and Warfare Reference Model (NCOW RM) and the GIG Architecture. Compact Disc (CD) copies of the GIG Architecture and NCOW RM are available through ASD(NII)/DOD CIO until its Web site is established. Additionally, IT and NSS systems must comply with current Information Assurance policies and procedures.

9. IT and NSS System-specific Policies. Current and newly established interoperability related policies that impact J-6 certifications are listed in Enclosure N.

ENCLOSURE B

RESPONSIBILITIES

1. The Joint Staff, J-6, will:

a. Conduct a capability interoperability certification of CDDs, CPDs and ISPs and other capabilities documents designated by the JROC, regardless of ACAT level.

b. Conduct a J-6 Functional Capability Board (FCB) Working Group assessment of all ICDs through the C2 FCB.

c. Conduct a J-6 FCB Working Group assessment of all Doctrine, Organization, Training, Material, Leadership, Personnel and Facility (DOTMLPF) Change Documents through the C2 FCB and other applicable FCBs.

d. Conduct supportability certification of IT and NSS for all ACAT.

e. Conduct interoperability system test validation of all IT and NSS for all ACAT, including Joint Interoperability System Certification, NCOW RM and KIP compliance and IA certification.

f. Coordinate IT and NSS interoperability and supportability policies, procedures and programs.

g. Monitor C2 R&D and acquisition of IT and NSS in collaboration with USD(AT&L), ASD(NII), and J-8 through the C2 FCB and other applicable FCBs.

h. Convene the MCEB consisting of the senior Service and agency officials responsible for communications-electronics matters and act as chairman (references h and v). The MCEB will consider interoperability and supportability matters referred to it by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. The board will:

(1) Act as the senior resolution body for issues related to IT and NSS, standards, interoperability testing and NR-KPP issues. All interoperability issues not resolved by these instructions and the MCEB may be referred to the Interoperability Senior Review Panel (ISRP) for final resolution.

(2) Obtain coordination for issues presented to the board among DOD components, between the Department of Defense and other governmental departments and agencies, and between the Department of Defense and representatives of foreign nations.

(3) Coordinate and furnish advice, guidance, direction, and assistance among components for IT and NSS interoperability and supportability matters.

(4) Establish the following sub-panels whose duties in regards to this instruction are as defined:

(a) The ITP will oversee conduct of the interoperability certification testing process, resolve testing issues, and waive requirements for Joint Interoperability Certification IAW MCEB Pub 1.

(b) The Information Assurance Panel (IAP) will resolve information assurance (IA) interoperability issues.

(c) The Interoperability Panel (IP) of the MCEB will resolve issues directly related to or involving IT and NSS systems interoperability, and operational and procedural standards.

i. Designate a POC to act as executive agent of the J-6 Assessment Tool (see Enclosure J).

j. Ensure that USD(AT&L), ASD(NII), and other DOD components have the opportunity to participate in or review the analysis conducted early to ensure that processes adequately address a sufficient range of interoperability issues and material approaches.

2. Joint Staff, J-2, will:

a. Designate J-2 document assessor points of contact (POCs) for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor POCs are responsible for the following J-6 Assessment Tool actions:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. The Intelligence Certification (led by DIA/J-2) of JCIDS documents is conducted in a separate, but related process that examines intelligence support needs for completeness, supportability, and impact on joint intelligence planning. Collaboration and coordination between J-2 and J-6 regarding issues relating to intelligence information requirements is critical to the respective goals of both processes. In addition, to conserve resources, coordination and combined testing with DISA JITC is encouraged to support security intelligence certification tests that overlap.

3. Joint Staff, J-4, will:

a. Designate J-4 document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor POCs are responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. Procedures and criteria for J-4 Certification of Insensitive Munitions are distinct from the procedures and criteria in this instruction and can be obtained through consultation with the Joint Staff J-4.

4. US Joint Forces Command (USJFCOM). Serves as the joint force integrator of the Department of Defense. USJFCOM, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the JBC ITDC. These demonstrations do not replace the JITC system interoperability test

certification. Demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

a. USJFCOM will review and confirm the sufficiency of NR-KPPs and integrated architectures for all IT and NSS programs for all ACAT, Non-ACAT, and fielded systems. This evaluation will be based on the warfighter's perspective using a universal joint task list (UJTL)/joint mission-essential task list (JMETL) based assessment process.

b. Designate command document assessor POCs for the J-6 Assessment Tool (Enclosure J). The command must have one primary and one alternate document assessor POC. The document assessor is responsible for the following J-6 Assessment Tool actions:

(1) Identify the individuals within the organization who should review each document.

(2) Assist each document reviewer in obtaining a username and password for a read only user account.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated organization approved reviewer comment matrix in the proper format.

5. Combatant commanders will:

a. Review and comment on relevant programs during the J-6 interoperability and supportability certification process.

b. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

c. Participate, as appropriate, in IT and NSS interoperability testing programs by planning, programming, budgeting, executing and providing resources IAW agreed-to schedules and test plans. Required interoperability testing and certification will have some impact on schedules and costs of programs. These cost and schedule impacts will need to be added to POM and project cost estimates.

6. Military Services, Defense agencies and US Special Operations Command (USSOCOM) will:

a. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

b. Identify all Service or Agency systems that require external joint and combined interfaces with other Service or agency programs and systems.

c. Ensure the CPD NR-KPP along with other KPPs and critical technical and operational issues are used to develop the ISP and the TEMP.

d. Ensure the Program Managers' design includes all user required external joint and combined DOD DISR-compliant system interfaces when building new systems or modifying existing ones through coordination with all DOD components and allies.

e. Participate in configuration management (CM) of interface standards.

f. Participate in DOD efforts to influence development of non-government standards for supportability of all IT and NSS. Implement standards in candidate systems and test those implementations for conformance with the standards.

g. Participate in the MCEB and appropriate sub-panels.

h. In coordination with DISA (JITC), develop interoperability test and evaluation criteria for inclusion in acquisition documents, TEMP, and other test plan submissions. Prior to a Milestone C decision approval for all new or modified IT and NSS, the Services and Defense agencies, and participating test unit coordinators will ensure those systems undergo Joint Interoperability Certification test and evaluation IAW these criteria. This includes any limited or prototype IOC fielding. Services, Defense agencies, and participating test unit coordinators will ensure a TEMP is approved, prior to KDP-C for space systems being acquired under reference dd, to ensure the system will complete interoperability certification testing IAW these criteria. Actual certification testing will likely occur after KDP-C and prior to the first launch and/or prior to declaration of IOC.

i. Participate in IT and NSS Joint interoperability and accreditation testing programs by planning, programming, budgeting, executing and providing resources in accordance with agreed-to schedules and test plans. Required Joint interoperability testing and certification will have some impact on schedules and costs of programs. These cost and schedule impacts will need to be added to POM and project cost estimates.

(1) Resources include:

(a) Services and Defense agencies, such as DISA JTIC.

(b) Services and Defense agencies systems, equipment, and personnel, necessary to accomplish standards conformance testing and interoperability testing.

(2) For DISA JITC system interoperability test certification, the sponsor will:

(a) Coordinate funding with DISA (JITC) prior to the initiation of DISA (JITC) efforts. The System Program Office will coordinate with DISA (JITC) to determine funding required to support interoperability testing and certification. Once funding is identified, the Program Office will identify this requirement as an integrated facet of the program cost through the Service/agency POM process.

(b) Include funding the Service/Agency Participating Test Unit Coordinator (PTUC). The PTUC will be the point of contact (POC) for coordinating funding with DISA (JITC) prior to the initiation of DISA (JITC) efforts.

j. Provide direction to acquisition managers to ensure that all weapon systems that have or depend on IT and NSS capabilities are certified and tested for interoperability.

k. Provide guidance to all program managers to ensure that information assurance hardware and software capabilities (tools) are assessed for and meet interoperability requirements as established by the IAP.

l. Ensure all programs are compliant with current DOD information assurance directives and policies.

m. Provide guidance and direction to all program managers that all systems must be certified and accredited IAW applicable policy.

n. Provide systems engineering guidance to other components to implement IA solutions and to facilitate IA accreditation.

7. Director, Defense Information Systems Agency (DISA) will:

a. Participate in the technical assessment of all IT and NSS requirements and capability documents.

b. Exercise DISA's role as executive agent for coordinating and integrating the common operating environment (COE), GIG, and GIG Enterprise Services (GIG-ES) activities.

c. Exercise DISA's role as executive agent for coordinating and integrating the Department of Defense IT standards activities, and for integrating the DOD DISR tenets and their supporting infrastructure activities and capabilities.

d. Manage the IT and NSS Standards within the Defense Standardization Program to ensure that appropriate standards are available and used. Ensure that requirements for standards are identified, and related standards projects are planned, prioritized and properly resourced.

e. Provide guidance, assistance, profiling tools and information on appropriate use of standards including the applicability of standards to

DOD DISR Services (e.g., networking), Domains (e.g., combat support) and program phases (e.g., use of existing standards for imminent acquisitions and use of emerging standards for long-range program planning).

f. Ensure that the DOD standards profiles (TV-1) conform to DOD DISR standards for interoperability by requiring that standards profiles be generated through the use of the DISR online tool and an interoperability requirements profile generated by the Levels of Information System Interoperability (LISI) InspecQtor tool.

g. Provide an assessment of the suitability of standards identified in IT and NSS programs submitted under this instruction. Standards issues that cannot be resolved will be forwarded by DISA to the MCEB.

h. Provide systems engineering and developmental interoperability testing assistance to system developers to help ensure maximum interoperability and minimum duplication.

i. Review all available Test and Evaluation Master Plans and provide acquisition managers with recommended interoperability test and evaluation criteria, as well as accreditation testing (reference u), for inclusion in acquisition documents and test plans. Coordinate with NSA regarding the inclusion of IA standards.

j. Establish and conduct, in collaboration with other DOD components, the JITC joint interoperability test and evaluation and certification program for IT systems, including NSS.

k. Forward Joint Interoperability System Test Certification results to the J-6 for validation IAW the NR-KPP validation.

l. Certify interoperability and standards implementation or compliance to the MCEB ITP and to the developmental and operational testing organizations of DOD components.

m. Publish an annual report to the Joint Staff J-6, USD(AT&L), ASD (NII/DOD CIO), DOT&E, DOD Executive Agent for Space, and USJFCOM containing a summary of system interoperability test certification status of functional areas.

n. IAW MCEB Pub 1, provide a semi-annual update in the status of DISA JITC interoperability testing to the MCEB.

o. Serve as executive agent for the MCEB ITP (reference h).

p. Coordinate with DIA in matters of networking and communications services for the DOD Intelligence Information System (DODIIS).

q. Facilitate joint interoperability across the DOD global, theater, and tactical network boundaries.

r. Provide systems engineering, planning, and program guidance to the DOD components and agencies to implement solutions and to facilitate joint interoperability.

s. Assist NSA/CSS in coordinating and defining tactical signals intelligence (SIGINT) standards and processes and promote security, integration, interoperability, and data sharing among systems. Additionally, in coordination with NSA, review and define information assurance standards.

t. Provide test tools and procedures, and support systems in support of interoperability and standards conformance testing. Validate test tools and procedures (including those developed by other organizations) for interoperability and standards conformance testing.

u. Designate a central office to act as system manager of the J-6 Assessment Tool (see Enclosure J).

v. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer obtain a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

w. Coordinate with the National Security Agency (NSA), for any DOD system that collects, stores, transmits, or processes unclassified or classified information, to ensure security-testing considerations are addressed in interoperability testing.

x. Establish and maintain an automated process to track system status, monitor certification status, document ICTO information, and track uncertified systems.

y. Exercise DISA's role as executive agent for the Joint Interoperability of Tactical Command and Control Systems (JINTACCS), Information Technology standardization program and conformance to current message implementations for all inter and intra DOD component IT and NSS that exchange and use information to enable units/forces to operate effectively in Joint, Coalition and interagency operations."

8. Community Functional Lead for Cryptology (CFLC) - Director, National Security Agency (NSA)/Chief Central Security Service (CSS), will:

a. As the executive agent for approving and enforcing tactical SIGINT architectures and standards, approve all SIGINT investment programs and provide standards compliance and interoperability assessment reports to assist MDAs in production decisions.

b. Ensure that DOD cryptologic/cryptographic programs and US Signals Intelligence Directives (USSIDs) comply with interoperability and supportability policy (e.g., DCID 6/1 and 6/3).

c. Ensure IA and IA-enabled products comply with National Security Telecommunications and Information Systems Security Policy 11 (NSTISSP 11).

d. Ensure, in coordination with other DOD components, that requirements for cryptologic/cryptographic systems interoperability are satisfied through the design and development of technical, procedural, and operational interfaces between IT and NSS systems and those intelligence systems processing foreign intelligence and foreign counterintelligence information.

e. Perform CM for cryptologic systems; perform CM jointly with DISA for the interface between cryptologic systems and IT and NSS systems.

f. Provide information assurance guidance and assistance to the development of information technology architectures, incorporation of information assurance related standards in the DOD Information Technology Standards Registry (DISR), and in certification and accreditation activities.

g. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

9. Director, National Geospatial-Intelligence Agency (NGA), will:

a. Ensure that National System for Geospatial Intelligence (NSGI) standards and specifications established by NIMA for geospatial intelligence support the interoperability of IT and NSS via coordination with the Military Services, DISA and the unified commands.

b. Set standards for all geospatial intelligence systems and interfaces, including to the Net Centric Enterprise Services and their accompanying KIPs.

c. Ensure NSGI standards and specifications incorporate imagery and geospatial information release or disclosure decisions.

d. Ensure that commercial and non-governmental standards used for imagery and geospatial systems and applications are open-systems based and conform to Defense Information Infrastructure (DII) and DOD DISR tenets for interoperability across the geospatial intelligence user community.

e. Designate document assessor POCs for the J-6 Assessment Tool (Enclosure J). Each organization will have one primary and one alternate document assessor POC. The document assessor is responsible for the following:

(1) Identify the individuals within the organization who should review each document being assessed on the tool.

(2) Assist each document reviewer in obtaining a username and password for a read only user account for the J-6 Assessment Tool.

(3) Staff the document internally to the document reviewers within the organization.

(4) Submit a consolidated reviewer comment matrix in the proper format to the J-6 Assessment Tool.

10. Director, Defense Intelligence Agency (DIA), will:

a. Ensure that standards and specifications established for measurement and signature intelligence (MASINT) under the US MASINT System (USMS) support the interoperability of IT and NSS systems via coordination with the Military Services.

b. Ensure that commercial and non-governmental standards used for MASINT systems and applications are open-systems based and conform to DII and DOD DISR tenets for interoperability.

11. Program Managers from combatant commands, Military Services and Defense agencies, when building new, or modifying existing systems, will ensure that they are:

a. Compliant with the Clinger-Cohen Act of 1996, as amended (sections replaced by Pub L 102-217).

b. Compliant with the latest version of the DOD Information Technology Standards Registry (DISR).

c. Certified and accredited IAW current DOD Information Assurance directives and policies.

d. Interoperable with other DOD, Joint and Coalition systems, unless security requirements prohibit or limit the sharing of information.

e. Properly evaluated and certified for interoperability by DISA or obtain an Interim Certificate to Operate (ICTO) IAW MCEB Pub 1, as required, until system interoperability test certification is complete.

f. Compliant with LISI profiles requirements.

12. DOD Executive Agent for Space. As the DOD executive agent for Space, the Under Secretary of the Air Force, will review and confirm the sufficiency of NR-KPPs and integrated architecture products for all National Security Space Programs for all ACAT, non-ACAT and fielded

systems. This evaluation will be based on ensuring architectures are in compliance with approved space architectures.

13. Other DOD Components. Coordinate on interoperability certification and supportability documents developed by other sponsors to identify opportunities for cross-component utilization, Joint Integration and harmonization of capabilities. Make recommendations to the J-6 on whether staffing documents contained in ICD, CDD, CPD, ISP proposals meet recognized standards.

(INTENTIONALLY BLANK)

ENCLOSURE C

PROCEDURES

1. General. The Joint Staff J-6 performs interoperability requirements certification, supportability certification and interoperability system validation for both the development and production of IT/NSS systems/programs. Documents submitted by Military Services and Defense agencies shall follow the format contained in CJCSM 3170.01 and shall include JCPAT system registration, LISI profiles (Enclosure K) and DISR online profiles (Enclosure L).

a. J-6 Capabilities Interoperability Certification. This certification occurs prior to each acquisition milestone.

(1) Initial Capabilities Document (ICD) certification occurs prior to Milestone A. ICD certification occurs prior to KDP-A for space systems being acquired under reference dd.

(2) Developmental Capabilities Interoperability Certification occurs prior to Milestone B usually in a CDD. Developmental certification allows the sponsor to adjust the KPP values in the next level document (typically, the CPD). For example, the timeliness fields within the IER matrix maybe "TBD" due to technology and spiral development. CDD certification occurs prior to KDP-B for space systems being acquired under reference dd.

(3) Production Capabilities Interoperability Certification occurs prior to Milestone C usually in a CPD. Production certification is more stringent than developmental certification. A complete design analogous to an ISP with all of the technical information and specifications is mandatory to ensure complete capabilities interoperability certification. CPD certification occurs prior to KDP-C for space systems being acquired under reference dd.

(4) The J-6 certifies the NR-KPP derived from a set of top-level requirements, capability documents and programs for all ACAT, non-ACAT, and fielded systems for conformance with policy, doctrine and applicable interoperability standards for joint IT and NSS. The J-6 forwards interoperability certification to the JROC or to the sponsoring DOD component via KM/DS.

(5) As part of the review process, J-8 staffs all JCIDS documents (to include JROC Interest, Joint Impact and Joint Integration) on KM/DS to OSD, combatant commanders, the Services, the Joint Staff and DOD agencies.

(6) USJFCOM, as the joint force integrator, will review ICDs, CDDs, CPDs and Information Support Plans (ISPs). USJFCOM, as the Chairman's Advocate for interoperability, may require selected programs and systems for interoperability demonstrations, using the JBC ITDC. Selection of the program or system may be made by the Joint Battle Management Command and Control Board of Directors. This does not replace the JITC system interoperability test certification and the demonstration results could be used or provided to JITC to assess the system for interoperability test certification.

(7) J-6 will forward unresolved interoperability issues to the MCEB or MIB for resolution. The MCEB or MIB will return resolved interoperability issues to the lead DOD component to complete the JROC approval process. The MCEB and MIB will ensure that unresolved issues resulting from interoperability assessments are presented to the JROC for resolution (see Figure C-1).

b. Supportability Certification. The J-6 certifies to ASD(NII) that IT and NSS programs for all ACAT, adequately address infrastructure requirements, the availability of bandwidth, spectrum support, and identify dependencies and interface requirements between systems. PMs will submit the applicable CDD/CPD along with the ISP into the JCPAT tool for supportability certification review.

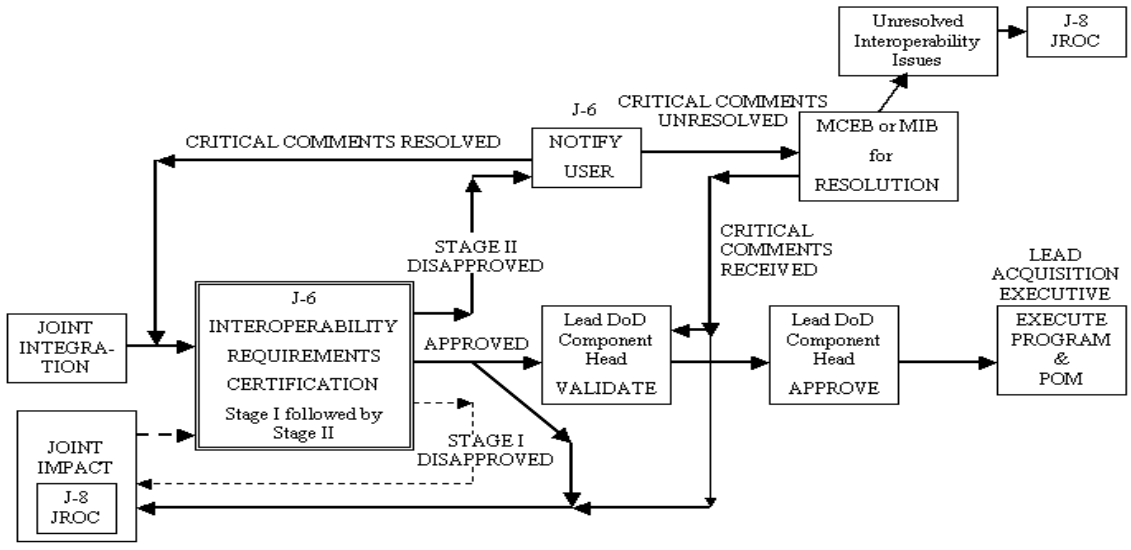

Figure I-1. Critical Comment Resolution Process

c. J-6 Interoperability System Validation. The J-6 validation is intended to provide total lifecycle oversight of warfighter capabilities interoperability. The J-6 validates the DISA (JITC) interoperability system test certification, which is based upon a joint certified NR-KPP, approved in the CDD, CPD and ISP. The validation will occur after receipt and analysis of the DISA (JITC) interoperability system test certification. The J-6 will issue an interoperability system certification memorandum to the respective Services, agencies and developmental and operational testing organizations.

2. Assessment Procedure Overview. Documents submitted by combatant commands/Services/agencies will be evaluated early in the lifecycle of a system and at all acquisition milestones to help the developer ensure that a system or program will successfully achieve system test certification and eventual fielding.

a. To support the interoperability certification process, J-6 requests technical assessments from DISA, Services and other DOD agencies.

b. USJFCOM, as the joint force integrator, will review all ICDs, CDDs, CPDs and ISPs.

c. Combatant commanders are invited to review and comment on all JCIDS documents during the J-8 (JROC) formal review. During this review, combatant commanders should review these documents for interoperability concerns and include interoperability related comments in the response to J-8. All interoperability comments submitted to the KM/DS tool will be identified in the KM/DS Comment Matrix by inserting “Interoperability Comment” as the first entry in the COMMENT column. Only comments so marked will be considered as part of the interoperability certification process.

d. J-8 staffs JCIDS documents using the J-8 KM/DS tool IAW references a and b. J-6 and OASD(NII) use a DISA-managed electronic tool, the ISP Program Assessment Tool in JCPAT, for the staffing, coordination, and compilation of assessment comments for ISPs. Enclosure J provides more information on the J-6 Assessment Tool.

e. J-6 interoperability certifications of capabilities and capability documents and programs are conducted in four distinct stages.

(1) O-6 Level Review is the draft assessment for all types of documents.

(2) Flag Level Review (for JROC Interest and Joint Impact JCIDS documents and OSD Special Interest ISPs) or Certification Review Stage (Joint Integration JCIDS documents and all non-OSD Special Interest ACAT ISPs) review is the final assessment.

(3) FCB Draft (JROC Interest and Joint Impact JCIDS documents) or Final stage (for Joint Integration JCIDS documents and all ISPs). Interoperability and supportability certifications will be issued upon successful adjudication of all comments from the previous two review stages. PMs will submit the final or FCB Draft document along with the adjudicated comments resolution matrix to the J-8 KM/DS tool (JCIDS documents) or JCPAT (ISPs) for review and certification by J-6.

(4) Upon receipt of the interoperability or supportability certification, PMs will post the completed and JROC/FCB or MDA approved document to KM/DS (JCIDS documents) or JCPAT (ISPs) for archival.

f. The suspense for completing Stage I documents for certification is normally 25 sequential days from the transmittal date from the J-8 RAD Action Officer (for JROC Interest and Joint Impact designated programs) for staffing in the J-8 KM/DS Tool. The suspense date for Joint Integration will normally be 25 sequential days from the date the Joint Potential Designator (JPD) is set by the JCIDS Gatekeeper (references a and b). DISA will download the applicable documents from KM/DS for all JROC Interest, Joint Impact and Joint Integration programs for interoperability and supportability review. The actual suspense date will be posted in the J-6 Assessment Tool.

g. The Stage II suspense is normally 21 sequential days.

h. The Stage III suspense is normally 15 sequential days after JROC or MDA approval.

i. All DOD ISP originators and assessors (combatant commanders, Services, agencies) will use the ISP Assessment Tool on JCPAT to submit ISP documents and assessor comments to J-6 for all ISPs.

j. During Stages I and II, assessors will submit comments in the following categories.

(1) CRITICAL. A critical comment indicates non-concurrence with the document until the comment is satisfactorily resolved. Prior to submitting a critical comment for flag-level review, a commenter is required to contact and coordinate with the document submitter and the comment will require a planner level approval for submission.

(2) SUBSTANTIVE. A substantive comment is provided because a section in the document appears to be or is potentially unnecessary, incorrect, misleading, confusing, or inconsistent with other sections. A substantive comment not resolved in Stage I could result in a critical comment during

Stage II. Additionally, multiple substantive comments could result in a critical comment and non-certification of the document.

(3) ADMINISTRATIVE. An administrative comment addresses what appears to be a typographical, format, or grammatical error.

k. Formal comments will indicate the page and paragraph numbers from the document and provide a rewrite recommendation and a rationale.

Org / Reviewer	Page #	Para #	Line #	Class (U,C,S)	Type (A,S,C)	Recommendation	Rationale	Comment
Joint Staff J-6 POC Name DSN: 999-9999 email@emailaddress.smil.mil or email@emailaddress.mil	0	0	0	U	C	Add sections 2, 3, 7, 9, and 14. Ensure all sections according to the instruction are titled correctly.	CJCSM 3170.01, Appendix A to Enclosure E.	General: Several sections missing.
Joint Staff J-6 POC Name DSN: 999-9999 email@emailaddress.smil.mil or email@emailaddress.mil	3	5.h	405	U	C	Include a SV-1 and narrative describing the systems and connectivity providing or supporting system functions. It should show how multiple systems link and integrate and identify key nodes including materiel system nodes, physical connections, association of systems to nodes, circuits, networks, warfighting platforms, and specific parameters, such as the mean time between failure, maintainability and availability.	CJCSI 3170; Mandatory contents of document	Systems Interface Description (SV-1) is missing.

Figure C-2. Sample Comments Resolution Matrix

ENCLOSURE D

CAPSTONE REQUIREMENTS DOCUMENT (CRD)

1. General.

a. The Capstone Requirements Document (CRD) contains capabilities-based requirements that facilitate the development of CDDs and CPDs by providing a common framework and operational concept to guide their development.

b. Until superseded, this enclosure describes the development of the I-KPP based on the integrated architecture products described in the DOD Architecture Framework (reference n) for CRD updates, and a NR-KPP based on NCOW RM compliance; integrated architecture products compliance, Key Interface Profiles and Information Assurance.

2. Applicability. The enclosure applies to CRDs submitted 6 months after publication of this instruction. The JROC will determine whether a CRD will contain the Interoperability Key Performance Parameter with Information Exchange Requirements (IERs) or an NR-KPP and its associated products. CRD sponsors will make a recommendation to the JROC when they present the CRD for validation and approval.

a. If a CRD is being updated, it must comply with the I-KPP based products. Paragraph 4 below details the steps for the development of a CRD based on the I-KPP.

b. If a new CRD is submitted, it must include the products based on the NR-KPP. Table A-2 outlines the principal NR-KPP products and paragraph 5 below details the steps for the development of a CRD based on the NR-KPP.

3. CRD Based on the I-KPP (see Table D-1)

a. Top-Level Interoperability Information Exchange Requirements (IERs).

(1) For CRDs, top-level IERs identify:

(a) **Who** are the information producers?

(b) **What** information is produced?

(c) **Why** the information is necessary?

(d) **Who** are the information consumers?

(e) **How** do the consumers make use of the information?

(2) Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission.

(3) A top-level IER matrix provided in a worksheet format will be part of CRDs when submitted.

(4) Top-level IERs may also be imported into modeling and evaluation tools including network warfare simulation (NETWARS) and other architecture planning and analysis systems.

(5) The top-level IER matrix must correlate with the proposed high-level operational concept graphic(s) and system interface description.

(6) A sample top-level IER matrix is illustrated in reference j, which provides detailed guidance for completing the matrix.

(7) In the development of the top-level IER matrix, the originator will determine if a given top-level IER is critical (top-level IER matrix field).

(8) A CRD critical top-level IER is an information exchange that is so a significant that if it does not occur the CRD mission area will be adversely impacted. IERs that must be flowed down to specific systems (ORDs) should be clearly specified in the CRD. An ORD critical top-level IER supports its associated CRD critical top-level IER, or will severely and adversely impact on a warfighter mission if not accomplished

b. Interoperability Key Performance Parameter

(1) CRD interoperability KPPs, and hence the IERs that the interoperability KPPs are derived from, will be measurable and testable.

Interoperability KPP	Threshold (T)	Objective (O)
All top-level IERs will be satisfied to the standards specified in the threshold (T) and objective (O) values.	100% of top-level IERs designated **critical**	100% of top-level IERs

Table D-1. Interoperability Threshold and Objective I-KPP

(2) Top-level IERs will be used as the basis to develop interoperability KPPs. The interoperability KPP definition will include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values.

(3) Typically the threshold criterion for the interoperability KPP will be100 percent accomplishment of the critical top-level IERs, and the objective criterion for the interoperability KPP will be the accomplishment of all top-level IERs.

4. CRD Interoperability I-KPP Development. All CRDs will have an interoperability KPP. The CRD interoperability KPP defines the level of interoperability required to be a part of the CRD Family of Systems (FoS) or System of Systems (SoS). The CRD interoperability KPP will use top-level IERs as the primary measure for interoperability and will outline the specific framework for CRD ORDs to follow. The following four-step methodology uses products from the DOD Architecture Framework and is recommended to develop CRD interoperability KPPs. If the CRD is being updated then the CRD will comply with the I-KPP based products. If the CRD is a new CRD it will have to produce products based on the NR-KPP. Table A-2 outlines the products.

a. **Step 1.** Identify **top-level** joint and combined information exchanges that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS, using a high-level operational concept graphic (OV-1).

b. **Step 2.** Document **top-level** joint and combined IERs that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS depicted in high-level operational concept graphic (OV-1) in an operational information exchange matrix (OV-3). Use matrix format illustrated in DOD Architecture Framework. Reference n provides additional guidance.

c. **Step 3.** Identify and label **critical** top-level IERs. A CRD critical Top-level IER is an information exchange that is so significant that if it

does not occur the CRD mission area will be adversely impacted. IERs that must be flowed down to specific systems (ORDs) should be clearly specified in the CRD. Critical top-level IERs will be required at threshold.

d. **Step 4.** Derive an interoperability KPP from the top-level IER matrix. A typical interoperability KPP is detailed below.

e. **Step 5.** Derive the NR-KPP from the top-level IER matrix. Document the NR-KPP in accordance with the definitions in Table D-1.

f. **Step 6.** Complete the CRD Crosswalk. It is possible for CRDs to interface or integrate with other CRDs. If so, then a crosswalk with other CRDs is applicable. The format for the crosswalk for a particular CRD is usually found in an appendix in the CRD. However, if the applicable CRD does not have a crosswalk, use the format shown in Table D-2 below. The following procedure is recommended:

(1) Identify possible CRDs the CRD must support. Assistance can be obtained from each CRD subject matter expert (SME). A list of approved CRDs with point of contact information is maintained at USJFCOM J-8 Requirements.

CRD Section Heading	CRD Page #	CRD Para #	Crosswalk Item	CRD/CDD/ CPD/ISP Page#	Para #	Line #	Yes/No/ NA
Interoperability							
Collaboration							

Table D-2. CRD Crosswalk Format

(2) List each CRD requirement that applies (Pg nr, par nr, and requirement title, (e.g., Interoperability, Sensor Coordination and Control, Combat ID, Reaction Time, etc.)).

(3). For each CRD requirement that applies, list the appropriate CRD KPP/operational requirement that the CRD requirement must demonstrate linkage and the contribution to (CRD Name, page number, paragraph number). This should be based on discussions between the office developing the CRD document and each applicable CRD subject matter expert.

g. Capstone Requirements Document Checklist (I-KPP Based). The following checklist is based on the requirements of the I-KPP and the CRD format from CJCSI 3170.01C. Document sponsors and assessors

should use this checklist.. Additionally, assessors must review the CRD from their specific viewpoint, concerns, and subject matter expertise.

No	CRD Para	Criteria	Reference
1.	App B	Does the CRD contain a high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
2.	App B	Does the high-level operational graphic(s) (OV-1) present a top-level view of the systems' interoperability requirements with other current and known future systems? CRD top-level IERs are information exchanges that are between systems that make up or are external to the combatant commanders, Services, agencies, allied, and coalition systems). The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will be used to show simple connectivity and can be annotated to show what information is exchanged.	CJCSI 6212.01C
3.	4	Was a top-level IER matrix (OV-3) provided in a worksheet format? Is the relationship between the exchanges in the matrix and the OV-1 annotated numerically?	CJCSM 3170.01
4.	4	Does the CRD top-level IER matrix (OV-3) contain all mandatory fields in the required format?	CJCSI 6212.01C
5.	4	Does the CRD top-level IER matrix (OV-3) correlate with the high-level operational graphic(s)?	CJCSI 6212.01C
6.	4	Does the CRD top-level IER matrix identify **who** are the information producers; **what** information is produced; **why** the information is necessary; **who** are the information consumers; **how** do the consumers make use of the information? Top-level IERs identify the elements of warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint mission area.	CJCSI 6212.01C
7.	4	Does the CRD I-KPP definition include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values?	CJCSI 6212.01C
8.	4	Does the CRD I-KPP threshold criteria include 100 percent accomplishment of the critical top-	CJCSI 6212.01C

No	CRD Para	Criteria	Reference
		level IERs?	
9.	4	Does the CRD I-KPP objective criteria include 100 percent accomplishment of the top-level IERs?	CJCSI 6212.01C
10.	4	Does the CRD include a requirement that applicable standards from the DOD DISR will be applied to ensure maximum interoperability?	CJCSI 3170.01C, CJCSI 6212.01C,
11.	4	Does the CRD address IERs between nodes of different classification?	CJCSI 6212.01C
12.	4	Does the CRD identify and include IA requirements?	CJCSI 6212.01C
13.	4	Does the CRD identify requirements, when applicable, for standardized software to ensure the needed level of interoperability?	CJCSI 6212.01C
14.	4	Does the CRD provide a compliance checklist for programs that fall under its scope?	CJCSM 3170.01C, CJCSI 6212.01C

Table D-3. J-6 Interoperability Certification and Assessment Criteria

Again, the above checklist is not all-inclusive. Assessors must also review the CRD from their specific viewpoint, concerns, and subject matter expertise.

5. CRD Interoperability based on NR-KPP (See Table D-5). All new CRDs will have a Net-Ready KPP (NR-KPP). The CRD NR-KPP defines the level of interoperability required to be a Net Centric. The CRD NR-KPP will use the documents and products prescribed in Table A-3 as the primary measure for interoperability and will outline the specific framework for NR-KPP CRD to follow. The following four-step methodology uses the NCOW RM and products from the DOD Architecture Framework and is required to develop CRD NR-KPPs.

a. **Step 1.** Identify joint and combined architectures that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS, using a high-level operational concept graphic (OV-1).

b. **Step 2.** Document joint and combined architectures that are between systems that make up the FoS or SoS, as well as those that are external to the FoS or SoS depicted in high-level operational concept graphic (OV-1) in an operational activity model (OV-5). Use matrix

format illustrated in DOD Architecture Framework. Reference n provides additional guidance.

c. **Step 3.** Identify and label critical activity interfaces, services, policy enforcement controls and datasharing. A critical interface, service, control or data sharing is so significant that if it does not occur the CRD mission area will be adversely impacted. Interfaces, services, policy enforcement controls and datasharing must be identified and be clearly specified in the CRD. Critical activities will be designated as threshold.

d. **Step 4.** Derive the Net-Ready KPP from requirements listed in from the products.

Net-Ready KPP	Threshold (T)	Objective (O)
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture**.	100percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture.

Table D-5. NR-KPP Threshold and Objective

e. **Step 5.** Derive the NR-KPP matrix. Document the NR-KPP in accordance with the definitions in Table D-5.

f. **Step 6.** Complete the CRD Crosswalk. It is possible for CRDs to interface or integrate with other CRDs. If so, then a crosswalk with other

CRDs is applicable. The format for the crosswalk for a particular CRD is usually found in an appendix in the CRD. However, if the applicable CRD does not have a crosswalk, use the format shown in Table D-6 below. The following procedure is recommended:

(1) Identify possible CRDs the CRD must support. Assistance can be obtained from each CRD subject matter expert (SME). A list of approved CRDs with point of contact information is maintained at USJFCOM J-8 Requirements.

CRD Section Heading	CRD Page #	CRD Para #	Crosswalk Item	CRD/CDD/ CPD/ISP Page#	Para #	Line #	Yes/No/ NA
Interoperability							
Collaboration							

Table D-2. CRD Crosswalk Format

(2) List each CRD requirement that applies (Pg nr, par nr, and requirement title, (e.g., Interoperability, Sensor Coordination and Control, Combat ID, Reaction Time, etc.)).

g. For each CRD requirement that applies, list the appropriate CRD KPP/operational requirement that the CRD requirement must demonstrate linkage and the contribution to (CRD Name, page number, paragraph number). This should be based on discussions between the office developing the CRD document and each applicable CRD subject matter expert.

h. Capstone Requirements Document Checklist (NR-KPP Based). The following checklist is based on the requirements of the NR-KPP and the CRD format from CJCSI 3170.01C. Document sponsors and assessors should use this checklist. Additionally, assessors must review the CRD from their specific viewpoint, concerns, and subject matter expertise.

No	**CRD Para**	**Criteria**	**Reference**
15.	App B	Does the CRD contain a high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
16.	App B	Does the high-level operational graphic(s) (OV-1) present a top-level view of the systems' interoperability requirements with other current and known future systems? CRD interfaces,	CJCSI 6212.01C

No	CRD Para	Criteria	Reference
		services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, that are between systems that make up or are external to the combatant commanders, Services, agencies, allied, and coalition systems). The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will be used to show simple connectivity and can be annotated to show what information is exchanged.	
17.	4	Was an operational activity model (OV-5) provided in a worksheet format? Are operational activities, relationships among activities, inputs and outputs. Overlays can show cost performing nodes, or other pertinent information between the OV-5and the OV-1 annotated numerically?	CJCSM 3170.01
18.	4	Does the CRD operational activity model (OV-5) contain all mandatory fields in the required format?	CJCSI 6212.01C
19.	4	Does the CRD operational activity model (OV-5) correlate with the high-level operational graphic(s)?	CJCSI 6212.01C
20.	4	Does the CRD operational activity model (OV-5) matrix identify **who** are the information producers; **what** information is produced; **why** the information is necessary; **who** are the information consumers; **how** do the consumers make use of the information? Top-level operational activity model (OV-5) identifies the elements of warfighter activities used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint mission area.	CJCSI 6212.01C
21.	4	Does the CRD NR-KPP definition include that all activity interfaces, services, policy-enforcement controls and datasharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products	CJCSI 6212.01C

No	CRD Para	Criteria	Reference
		(including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values will be satisfied to the standards specified in the threshold and objective values?	
22.	4	Does the CRD I-KPP threshold criteria include 100 percent accomplishment of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements designated as enterprise-level or critical in the Joint integrated architecture?	CJCSI 6212.01C
23.	4	Does the CRD I-KPP objective criteria include 100 percent accomplishment 100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing requirements in the Joint integrated architecture?	CJCSI 6212.01C
24.	4	Does the CRD include a requirement that applicable standards from the DOD DISR will be applied to ensure maximum interoperability?	CJCSI 3170.01C, CJCSI 6212.01C,
25.	4	Does the CRD identify and include IA requirements?	CJCSI 6212.01C
26.	4	Does the CRD identify requirements, when applicable, for standardized software to ensure the needed level of interoperability?	CJCSI 6212.01C
27.	4	Does the CRD provide a compliance checklist for programs that fall under its scope?	CJCSM 3170.01C, CJCSI 6212.01C

Table D-5. J-6 Interoperability Certification and Assessment Criteria

Again, the above checklist is not all-inclusive. Assessors must also review the CRD from their specific viewpoint, concerns and subject matter expertise.

ENCLOSURE E

INITIAL CAPABILITES DOCUMENT (ICD)

1. General

a. The Initial Capabilities Document (ICD) describes capability gaps that exist in joint warfighting functions as described in the applicable joint concepts and integrated architectures. The ICD defines the capability gap in terms of the functional area, the relevant Range of Military Operations, and time. The ICD must capture the results of a well-framed functional analysis, as described in reference a.

b. There is no requirement for J-6 to issue interoperability requirements certifications for ICDs; however, during the validation and approval process, J-6 will review the proposed architecture for compliance with the interoperability standards listed in reference l. ICDs are approved through the JCIDS process IAW reference a.

2. Applicability. This enclosure applies to all ICDs regardless of ACAT, approval authority, designation, increment, or block. ICDs will comply with requirements indicated in table A-1.

3. ICD Interoperability Implications. ICDs will document interoperability and information assurance in the mandatory architecture views and description in appendix A of the ICD.

a. The OV-1 is the only mandatory architecture view in an ICD IAW reference a. The format for each view will be IAW reference j or its replacement.

b. A short description of the view, its intended use and a discussion of the top-level exchanges will accompany the OV-1 view. The narrative for each view should be as concise as possible while still giving the necessary explanation of the view. A length of ½ page or less is ideal; some views may require a longer narrative.

4. ICD Interoperability Checklist. Table E-1 below provides detailed interoperability standards assessment criteria for the ICD.

No	ICD Para	Criteria	Reference
1		Does the ICD include an OV-1?	CJCSI 3170.01C
2		Does the operational graphics include a complete description that completely describes the architecture, its intended use, and discuss the top-level exchanges depicted in the view?	CJCSI 6212.01C
3		Do the operational graphics provide traceability between each graphic?	CJCSI 6212.01C
4		Does the high-level operational graphic(s) (OV-1) present a top-level view of the system's interoperability requirements with other current and known future systems? The focus of the graphic is to present a top-level view of the system's interoperability requirements with other current, and known future systems. Top-level is that level of detail required to graphically illustrate how the new system exchanges information between other combatant commanders, Services, agencies, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will show simple connectivity and can be annotated to show what information is exchanged.	CJCSI 6212.01C
5		Does the ICD high-level operational graphic(s) (OV-1) correlate with the associated CRD high-level operational graphic(s) (OV-1)?	CJCSI 6212.01C
6		Does the ICD include a statement of compliance with the most current version of the DOD DISR?	CJCSI 6212.01C

Table E-1. ICD Interoperability Standards Assessment Criteria

5. Net Centric Assessment Criteria. Table E-2 below provides criteria to assist program managers to characterize the net-centric attributes of their services and data products. This characterization will assist Domain Managers to determine which programs should be transformed, sustained, or eliminated and to identify new starts.

Question		Description	Map to Checklist
General Information [establishes the general context of the system for analysis]			
1.	Which domain(s) is the program a member? If multiple domains, which is primary? Which capabilities does the program provide?	This should be one or more of the business or warfighting domains. **Warfighter** — Battlespace Awareness; Command and Control; Force Application; Protection; Focused Logistics **Business** — Logistics; Acquisition/Procurement; Finance, Accounting Operations, Programming, Budgeting and Funds Control; Real Property & Environmental Liabilities; Human Resources This should give an indication of the scope of program, e.g., Army payroll processing, weapons targeting, etc.	N/A
2.	What edge devices do the program support/or is programmed to support?	This identifies the minimum expected physical computing capabilities of the users, e.g., PDAs, radios, desktop computers, etc.	N/A
3.	What is current and projected subscriber population?	This would indicate anticipated/known user base, e.g., entire Department, Navy, single ship, 500 OSD personnel, federal and local agencies, commercial businesses, coalition/foreign nationals, etc.	N/A

Question		Description	Map to Checklist
4.	How does/will the program support weakly connected (e.g., "disadvantaged") users?	This looks for support to low bandwidth users or intermittently connected users, e.g., thin client applications, compression technologies, subscription services, etc.	N/A
Architecture			
5.	Which DOD integrated architecture is the program compliant?	DISR, DOD Arch. Framework**,** NCOW, COE, NMCI, other?	N/A
6.	Which of the NCOW RM emerging protocol standards does/will the program use?	The Net Centric Operations and Warfare – Reference Model (NCOW RM) Technical View-2 standards URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/index.htm	N/A
7.	Is the program IP-network enabled? Does it implement [programmed to] IPv4 and IPv6?	The policy is to implement IPv6, but to support IPv4 until IPv6 is implemented.	IP
Services			

Question		Description	Map to Checklist
8.	Which enterprise services in the NCOW RM, Operational View-5, does the program provide or is programmed to provide? How does the program provide [plan to] advertise the services? Schedule?	This would indicate the types of services that are provided, e.g., discovery service, mediation service, etc., which are becoming the standard as defined by the GIG ES Capabilities Development Document (CDD). URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/main.htm Addressing "how program provides services" should describe architecture, what technologies are being used (e.g., Web Services Definition Language [WSDL]), whether the service is registered and catalogued so it can be discovered by the Enterprise or other COIs, and whether service interfaces are defined.	Application diversity, OHIO (only handle information once)
9.	What services in the NCOW RM does the program access [plan to access] that are provided by others? How does the program access [plan to access] the services? Schedule?	This should indicate what Core Enterprise Services or Domain or COI services program uses, e.g., NCES discovery service, C2 targeting service, etc., that are becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]. Addressing "how program access" should identify necessary interfaces, technologies.	Data centric

Question		Description	Map to Checklist
10.	What other services do the program provide [programmed to provide]? How does the program provide [plan to provide] the services? Schedule?	This would identify any other services that are being offered and the approach to implementing them, e.g., application services that are becoming the standard as defined by the GIG ES CDD.	Data centric, Application diversity
11.	To whom does the program offer [plan to offer] services (e.g., entire DOD Enterprise, subscribers' base, a COI?)	This indicates whether the program is developing services for its own exclusive use or as shareable services for others.	Apps on the Web
12.	Does the program have or plans to commit to a Service Level Agreement (SLA)?	This commits a program to delivering the level of service specified in the SLA and provides external users a level of expectation.	QoS
13.	Will the program use the common service for Identification and Authorization?	To identify whether these functions are projected to be stove-piped and local to the program, common to the COI/Domain or provided by a common service.	Application diversity
Data Aspects			

Question		Description	Map to Checklist
14.	What data does the program generate and make available to the Enterprise or Communities of Interest? What processing does the program perform prior to posting the data? Is the program data a primary source or authoritative data?	Indicate which data assets (information products) will be shared with the Enterprise or within or outside program domain, e.g., databases, target tracks, UAV video feeds, etc. Also, indicate at what points in program data processing that the data will be made available, e.g., raw imagery, enhanced imagery, or enhanced imagery overlaid with troop locations. This indicates whether the data is the source or a copy of the primary source (duplicated).	OHIO, Post in parallel
15.	How does program advertise or plan to advertise its data (make it discoverable)? What is the plan to advertise in the future if the program is not using a registry today? When?	This indicates that discovery metadata is being generated for that data (compliant with DOD Discovery Metadata Spec that is becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]), the level of granularity for which discovery metadata is provided (e.g., metadata created for an entire database vs. individual records); the existence of a catalog, etc.	Data centric

Question		Description	Map to Checklist
16.	How does program make or plan to make that data available to other users?	This should address how the data will be made accessible to users on the network (e.g., storage accessible on the network, Web services that expose the application data). Must also indicate whether data access will be restricted based on security accesses. This should also describe the technique used to bind the requestor to the service (e.g., Web Services Definition Language [WSDL]).	Data centric, OHIO
17.	How does the program provide or plan to provide information about program data so that it can be accessed? If not using the DOD Metadata Registry and Clearing House, what is the plan to do so and when?	This would identify what metadata is being registered in the DOD Metadata Registry (main or federated registry), e.g., taxonomies, data dictionaries, schemas, etc	Data centric
18.	What percentage of the program's data is or will be available to other Domains/COIs?	This indicates the degree to which a program's data is accessible/shared.	Data centric, OHIO
Application			

Question		Description	Map to Checklist
19.	Is the system NCOW compliant? Is the system registered on the net for discovery? If not, what is the schedule?	Users can discover and use the system for data manipulation or collaboration.	Application diversity
IA/Security			
20.	What security domain does/will the program support?	Compartmented, SCI, TS, SECRET, and FOUO, Unclass?	N/A
21.	How does or will program authenticate the service requestor at the transport layer? How does/will program mediate security assertions (to pass security related information between systems, processes, and domains)? What architectural options are/will be used to provide "defense in depth" in the service-oriented architecture?	This would describe how the security context is extended from the request originator to the service application. This would define the method/standards being used to insert security assertions into the requesting message (e.g., Security Assertions Markup Language [SAML]) This would define whether XML gateways/firewalls are used, the use of Public Key Infrastructure (PKI), SAML-in-SOAP (Simple Object Access Protocol), or whether the service application itself is used to implement XML-signature, XML-encryption, etc.	Dynamic allocation of access

Question		Description	Map to Checklist
22.	What data does/will the program need to exchange across security domains (e.g., email, structured data sets, unstructured documents, imagery, etc.)? How does/will the program accomplish or plan to accomplish the exchange? Is this mechanism/capability inherent in the program or dependent upon some other program for this capability and if known, which program?	Indicate the type of data to be exchanged and its classifications and/or handling caveats. Indicate between which security domains it will be exchanged (one way/both ways) and type of cross-domain solution (e.g. guard) used.	Application diversity, Dynamic allocation of access
23.	If the program's IA/security services were not described in the Services section of this questionnaire, how does or will the program manage identity and privileges?	Indicate whether the product or service will confirm identity of users and processes through PKI certificates. Will the product or service be access-controlled or open to all users?	Dynamic allocation of access

Question		Description	Map to Checklist
24.	Is your program compliant with the IA component of the GIG Architecture?	This addresses whether a program is aware of the need to comply with the IA architecture component.	Dynamic allocation of access

Table E-2. Net Centric Assessment Criteria

(INTENTIONALLY BLANK)

ENCLOSURE F

NET-READY KEY PERFORMANCE PARAMETER FOR THE CAPABILITY DEVELOPMENT DOCUMENT (CDD)

1. General. The Capability Development Document (CDD) is the warfighter's primary means of providing authoritative, measurable and testable requirements for the system development and demonstration (SDD) phase of an acquisition program. The CDD is guided by the Initial Capabilities Document (ICD), applicable CRDs, the Analysis of Alternatives (AoA), and the Technology Development Strategy, and captures the information necessary to deliver a system using mature technology in a specific increment within an acquisition strategy. In addition, writers of CDDs are reminded that there are special policies that impact J-6 interoperability certifications. Where appropriate, the following topics from Table F-2 must be addressed in the CDD:

a. Electromagnetic Environmental Effects and Spectrum Supportability

b. Host-nation Approval (HNA)

c. Selective Availability Anti-Spoofing Module (SAASM)

d. Information Assurance

2. Applicability. This enclosure applies to all CDDs regardless of ACAT, fielded status, approval authority, designation, increment, or block.

3. CDD Net-Ready Key Performance Parameter. All CDDs that exchange information will have a NR-KPP. At this point in the design (Developmental), there is an acceptable risk of incomplete architectural information. (i.e. incomplete timeliness in the OV-2) The CDD NR-KPP is derived from a completed architecture and developed from the below mandatory architecture products.

a. AV-1, OV-2, OV-4, OV-5, OV-6C

b. SV-4, SV-5, SV-6

c. TV-1 generated from DISR online

d. Applicable CRD crosswalk (See Table D-3)

e. Initial LISI Profile (Interface Requirements Profile) See Enclosure K

f. NR-KPP statement (Table F-1)

g. IA Statement of Compliance

h. Key Interface Profile (KIP) Declaration (list of KIPs that apply to system)

4. The CDD NR-KPP defines the interoperability requirements for the proposed system. The CDD NR-KPP will be derived from a completed integrated architecture that characterizes the performance of the proposed system.

5. Information Assurance. Information assurance is an integral part of net readiness. The NR-KPP description must include how the system will implement information assurance policies and procedures IAW the most current policies and procedures. If public key infrastructure (PKI) technology is required, a statement that PKI technology will be acquired as part of this effort and will be installed and used, including in initial fielding efforts, to ensure information security over all voice, video, and data transmission.

6. Standards. To further ensure interoperability among systems all IT and NSS systems shall comply with the most current version of the DOD DISR as a common set of standards. The DISR online will help the user build a DOD DISR-compliant standards profile (TV-1).

7. LISI Interface Requirements Profile. System interface requirements should be captured using the INSPECQTOR tool. See Enclosure J.

8. CDD NR-KPP Development. Development of the NR-KPP begins with designing the architecture for the proposed system. Without an architecture, the systems will not meet its goals, or meet any interoperability requirements. Each architecture view has a purpose that can be traced back to an operational concept.

a. **Step 1.** Develop the mandatory architecture views. Ideally, the CDD architecture views should be very much the same as the ICD except with more detail.

(1) The format and description for all of the architectural views will be IAW with the most current version of reference n. All the fields/columns for each architecture view from reference n are mandatory.

(2) A short description of the view, its intended use and a discussion of the top-level exchanges will accompany each view. The narrative for each view should be as concise as possible while still giving the necessary explanation of the view. A length of ½ page or less is ideal; some views may require a longer narrative.

b. **Step 2**. Complete the CRD Crosswalk. The format for the crosswalk for a particular CRD is usually found in an appendix of the applicable CRD. However, if the applicable CRD does not have a crosswalk, use the format shown in Table D-3.

c. **Step 3**. Build a DISR online standards profile (TV-1). This profile is required prior to submitting the CDD.

d. **Step 4**. Complete the initial LISI profile (Interface Requirement Profile) using the INSPECQTOR tool. This profile is required prior to submitting the CDD. See Enclosure K.

e. **Step 5**. Include the NR-KPP statement. The NR-KPP definition statement will document that all requirements will be satisfied to the standards specified in the threshold and objective values. The NR-KPP statement alone does not ensure interoperability requirements; a system must also be designed against the appropriate architectures, most current version of the DOD DISR and IA standards.

KPP	**Threshold**	**Objective**
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture.

Table F-1. CDD NR-KPP Statement

* Data processing is defined as: The input, output, verification, organization, storage, retrieval, transformation and extraction of information from data.

f. **Step 6.** Include the Key Interface Profile (KIP) Declaration. The declaration is the list of the KIPs that apply to the system. The KIPs declaration alone does not ensure interoperability; a system must also be designed against the appropriate architectures, most current version of the DOD DISR and IA standards.

g. **Step 7.** Include an IA statement of compliance reading, " This system is currently in full compliance with DOD Directive 8500.1 and DOD Instruction 8500.2, and with Phase 1 Definition of the DITSCAP (DOD Instruction 8500.40), and has made the required Information Assurance documentation available to the Joint Staff J-6 for review."

9. CDD Assessment Criteria. Table F-2 below provides criteria to assist assessors in reviewing a CDD in support of the J-6 Interoperability Requirements Certification.

No	CDD Para	Criteria	Reference
1.		Does the CDD include top-level graphic(s) OV-2, OV-4, OV-5, and OV-6C?	CJCSI 6212.01C
2.		Does the CDD include top-level systems graphics-SV-1 (or SV-2 in the case of network systems), and SV-4, SV-5, and SV-6?	CJCSI 6212.01C
3.		Do the architecture graphics include a short description that completely describes the architecture, its intended use, and discusses the top-level exchanges depicted in the view?	CJCSI 6212.01C
4.		Are the architecture graphics traceable between each view?	CJCSI 6212.01C
5.		Do the architecture graphics present a top-level view of the system's interoperability requirements with other current and known future systems? The focus of the graphics is to present a top-level view of the system's interoperability requirements with other current, and known future systems. Top-level is that level of detail required to graphically illustrate how the new system exchanges information between other combatant commanders, Services, agencies, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will show simple connectivity and can be annotated to show	CJCSI 6212.01C

No	CDD Para	Criteria	Reference
		what information is exchanged.	
6.		Do the CDD architecture graphics correlate with the associated CRD architecture graphics?	CJCSI 6212.01C
7.		Do the architecture mandatory views contain all mandatory fields in the required format?	CJCSI 6212.01C
8.		Does the CDD identify the interfaces for the system for each mission area that the system is proposed to support (e.g., CAS, AAW, surveillance, and reconnaissance)?	CJCSI 3170.01
9.		Do the CDD NR-KPP definitions include all appropriate elements of the associated CRD NR-KPP?	CJCSI 6212.01C
10.		Does the CDD system architecture view identify specific current and known IT and NSS sub-systems and interfaces that need to exchange information? The system interface description links together the operational and systems architecture views by depicting the assignments of subsystems and their interfaces to the systems and needlines described in the high level operational graphic diagram.	CJCSI 6212.01C
11.		Does the CDD describe considerations for joint, combined, and coalition use?	CJCSI 3170.01
12.		Does the CDD identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO, and other allied and friendly nation systems?	CJCSI 3170.01
13.		Does the CDD require the system to comply with applicable information technology standards contained in the current DOD DISR?	CJCSI 6212.01
14.		If PKI is required, does the CDD include a statement that public key infrastructure (PKI) technology will be acquired as part of this effort and will be installed and used, including in initial fielding efforts, to ensure information security over all voice, video, and data transmission? PKI implementation should also consider communications interoperability with commercial and multinational partners.	CJCSI 6212.01C
15.		Does the CDD address the interconnection of systems operating at different classification levels? What information assurance concepts does your program implement?	CJCSI 3170.01

No	CDD Para	Criteria	Reference
16.		Does the CDD identify a requirement for spectrum supportability?	CJCSI 6212.01
17.		Does the CDD address electromagnetic environment effects (E3)?	CJCSI 6212.01
18.		Does the CDD identify requirements for radio-based communications that will be satisfied by the joint tactical radio system (JTRS) CDD?	CJCSI 6212.01C
19.		Does the system identify requirements for data correctness, data availability and data processing (one method: the Integrated Architecture Behavior Model)?	CJCSI 6212.01C
20.		Does the CDD include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the CDD clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment after 1 October 2002?	CJCSI 6212.01C
21.		Does the CDD adequately address the requirement for interoperability system testing and certification?	CJCSI 6212.01
22.		Does the CDD contain a DISR online standards profile (TV-1)?	CJCSI 6212.01
23.		Does the CDD contain an initial LISI Interface Requirements profile?	CJCSI 6212.01
24.		Does the CDD contain a KIP Declaration?	CJCSI 6212.01

Table F-2. CDD – J-6 Interoperability Certification and Assessment Criteria

10. Net Centric Assessment Criteria. Table F-3 below provides criteria to assist program managers to characterize the net-centric attributes of their services and data products. This characterization will assist Domain Managers to determine which programs should be transformed, sustained, or eliminated and to identify new starts.

Question	Description	Map to Checklist
General Information [establishes the general context of the system for analysis]		

Question		Description	Map to Checklist
1.	Which domain(s) is the program a member? If multiple domains, which is primary? Which capabilities does the program provide?	This should be one or more of the business or warfighting domains. **Warfighter** — Battlespace Awareness; Command and Control; Force Application; Protection; Focused Logistics **Business** — Logistics; Acquisition/Procurement; Finance, Accounting Operations, Programming, Budgeting and Funds Control; Real Property & Environmental Liabilities; Human Resources This should give an indication of the scope of program, e.g., Army payroll processing, weapons targeting, etc.	N/A
2.	What edge devices do the program support/or is programmed to support?	This identifies the minimum expected physical computing capabilities of the users, e.g., PDAs, radios, desktop computers, etc.	N/A
3.	What is current and projected subscriber population?	This would indicate anticipated/known user base, e.g., entire Department, Navy, single ship, 500 OSD personnel, federal and local agencies, commercial businesses, coalition/foreign nationals, etc.	N/A

Question		Description	Map to Checklist
4.	How does/will the program support weakly connected (e.g., "disadvantaged") users?	This looks for support to low bandwidth users or intermittently connected users, e.g., thin client applications, compression technologies, subscription services, etc.	N/A
Architecture			
5.	Which DOD integrated architecture is the program compliant?	DISR, DOD Arch. Framework**,** NCOW, COE, NMCI, other?	N/A
6.	Which of the NCOW RM emerging protocol standards does/will the program use?	The Net Centric Operations and Warfare – Reference Model (NCOW RM) Technical View-2 standards URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/index.htm	N/A
7.	Is the program IP-network enabled? Does it implement [programmed to] IPv4 and IPv6?	The policy is to implement IPv6, but to support IPv4 until IPv6 is implemented.	IP
Services			

Question		Description	Map to Checklist
8.	Which enterprise services in the NCOW RM, Operational View-5, does the program provide or is programmed to provide? How does the program provide [plan to] advertise the services? Schedule?	This would indicate the types of services that are provided, e.g., discovery service, mediation service, etc., which are becoming the standard as defined by the GIG ES Capabilities Development Document (CDD). URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/main.htm Addressing "how program provides services" should describe architecture, what technologies are being used (e.g., Web Services Definition Language [WSDL]), whether the service is registered and catalogued so it can be discovered by the Enterprise or other COIs, and whether service interfaces are defined.	Application diversity, OHIO
9.	What services in the NCOW RM does the program access [plan to access] that are provided by others? How does the program access [plan to access] the services? Schedule?	This should indicate what Core Enterprise Services or Domain or COI services program uses, e.g., NCES discovery service, C2 targeting service, etc., that are becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]. Addressing "how program access" should identify necessary interfaces, technologies.	Data centric

Question		Description	Map to Checklist
10.	What other services do the program provide [programmed to provide]? How does the program provide [plan to provide] the services? Schedule?	This would identify any other services that are being offered and the approach to implementing them, e.g., application services that are becoming the standard as defined by the GIG ES CDD.	Data centric, Application diversity
11.	To whom does the program offer [plan to offer] services (e.g., entire DOD Enterprise, subscribers' base, a COI?)	This indicates whether the program is developing services for its own exclusive use or as shareable services for others.	Apps on the Web
12.	Does the program have or plan to commit to a Service Level Agreement (SLA)?	This commits a program to delivering the level of service specified in the SLA and provides external users a level of expectation.	Quality of Service
13.	Will the program use the common service for Identification and Authorization?	To identify whether these functions are projected to be stove-piped and local to the program, common to the COI/Domain or provided by a common service.	Application diversity
Data Aspects			

Question		Description	Map to Checklist
14.	What data does the program generate and make available to the Enterprise or Communities of Interest? What processing does the program perform prior to posting the data? Is the program data a primary source or authoritative data?	Indicate which data assets (information products) will be shared with the Enterprise or within or outside program domain, e.g., databases, target tracks, UAV video feeds, etc. Also, indicate at what points in program data processing that the data will be made available, e.g., raw imagery, enhanced imagery, or enhanced imagery overlaid with troop locations. This indicates whether the data is the source or a copy of the primary source (duplicated).	OHIO, Post in parallel
15.	How does program advertise or plan to advertise its data (make it discoverable)? What is the plan to advertise in the future if the program is not using a registry today? When?	This indicates that discovery metadata is being generated for that data (compliant with DOD Discovery Metadata Spec that is becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]), the level of granularity for which discovery metadata is provided (e.g., metadata created for an entire database vs. individual records); the existence of a catalog, etc.	Data centric

Question		Description	Map to Checklist
16.	How does program make or plan to make that data available to other users?	This should address how the data will be made accessible to users on the network (e.g., storage accessible on the network, Web services that expose the application data). Must also indicate whether data access will be restricted based on security accesses. This should also describe the technique used to bind the requestor to the service (e.g., Web Services Definition Language [WSDL]).	Data centric, OHIO
17.	How does the program provide or plan to provide information about program data so that it can be accessed? If not using the DOD Metadata Registry and Clearing House, what is the plan to do so and when?	This would identify what metadata is being registered in the DOD Metadata Registry (main or federated registry), e.g., taxonomies, data dictionaries, schemas, etc	Data centric
18.	What percentage of the program's data is or will be available to other Domains/COIs?	This indicates the degree to which a program's data is accessible/shared.	Data centric, OHIO
Application			

Question		Description	Map to Checklist
19.	Is the system NCOW compliant? Is the system registered on the net for discovery? If not, what is the schedule?	Users can discover and use the system for data manipulation or collaboration.	Application diversity
IA/Security			
20.	What security domain does/will the program support?	Compartmented, SCI, TS, SECRET, and FOUO, Unclass?	N/A
21.	How does or will program authenticate the service requestor at the transport layer? How does/will program mediate security assertions (to pass security related information between systems, processes, and domains)? What architectural options are/will be used to provide "defense in depth" in the service-oriented architecture?	This would describe how the security context is extended from the request originator to the service application. This would define the method/standards being used to insert security assertions into the requesting message (e.g., Security Assertions Markup Language [SAML]) This would define whether XML gateways/firewalls are used, the use of Public Key Infrastructure (PKI), SAML-in-SOAP (Simple Object Access Protocol), or whether the service application itself is used to implement XML-signature, XML-encryption, etc.	Dynamic allocation of access

Question		Description	Map to Checklist
22.	What data does/will the program need to exchange across security domains (e.g., email, structured data sets, unstructured documents, imagery, etc.)? How does/will the program accomplish or plan to accomplish the exchange? Is this mechanism/capability inherent in the program or dependent upon some other program for this capability and if known, which program?	Indicate the type of data to be exchanged and its classifications and/or handling caveats. Indicate between which security domains it will be exchanged (one way/both ways) and type of cross-domain solution (e.g., guard) used.	Application diversity, Dynamic allocation of access
23.	If the program's IA/security services were not described in the Services section of this questionnaire, how does or will the program manage identity and privileges?	Indicate whether the product or service will confirm identity of users and processes through PKI certificates. Will the product or service be access-controlled or open to all users?	Dynamic allocation of access

Question		Description	Map to Checklist
24.	Is your program compliant with the IA component of the GIG Architecture?	This addresses whether a program is aware of the need to comply with the IA architecture component.	Dynamic allocation of access

Table F-3. Net Centric Assessment Criteria

(INTENTIONALLY BLANK)

ENCLOSURE G

NET READY KEY PERFORMANCE PARAMETER FOR THE CAPABILITY PRODUCTION DOCUMENT (CPD)

1. General. The Capability Production Document (CPD) is the warfighter's primary means of providing authoritative, measurable and testable requirements for the production/fielding phase of an acquisition program. A CPD is finalized after critical design review and is validated and approved prior to the Milestone C acquisition decision. The CPD is guided by the Initial Capabilities Document (ICD), applicable CRDs, the Capability Development Document (CDD), developmental testing results, and critical design review. It captures the information necessary to support production of an increment within an acquisition strategy. This enclosure describes development of the NR-KPP for the Capability Production Document. In addition, writers of CPDs are reminded that there are special policies that impact J-6 interoperability certifications. Where appropriate, the following topics from Table F-2 must be addressed in the CPD:

a. Electromagnetic Environmental Effects and Spectrum Supportability

b. Host-nation Approval (HNA)

c. Selective Availability Anti-Spoofing Module (SAASM)

d. Information Assurance

2. Applicability. This enclosure applies to all CPDs regardless of ACAT, fielded status, approval authority, designation, increment, or block.

3. CPD Net-Ready Key Performance Parameter. All CPDs that exchange information will have NR-KPP. CPDs that come under the umbrella of a CRD must ensure compliance with the CRD NR-KPP (reference a) for those capabilities common to both the CPD system and the CRD. It is mandatory at this point in design of the system that the NR-KPP is completely measurable. The CPD NR-KPP is derived from a completed architecture and developed from the below mandatory architecture products:

a. AV-1, OV-2, OV-4, OV-5, OV-6C

b. SV-4, SV-5, SV-6

c. TV-1 generated from DISR online

d. Applicable CRD crosswalk (See Table D-3)

e. Complete LISI Profile (Interoperability Profile). See Enclosure K.

f. NR-KPP statement. (Table G-1)

g. IA Statement of Compliance

h. Key Interface Profile (KIP) Declaration (list of the KIPs that apply to the system)

4. CPD NR-KPP Development. Development of the NR-KPP begins with designing the architecture for the proposed system. Without an architecture the systems will not meet its goals nor meet any interoperability requirements. Each architecture view has a purpose that can be traced back to the operational concept.

a. **Step 1**. Develop the mandatory architecture views. Ideally, the CPD architecture views should be very much the same as the CDD except with more detail.

(1) The format and description for all of the architectural views will be IAW with the most current version of the DOD Architecture Framework (reference n). (All of the fields/columns for each architecture view from reference n are mandatory.)

(2) A short description of the view, its intended use and a discussion of the top-level exchanges will accompany each view. The narrative for each view should be as concise as possible while still giving the necessary explanation of the view. A length of ½ page or less is ideal; some views may require a longer narrative.

b. **Step 2.** Complete the CRD Crosswalk. The format for the crosswalk for a particular CRD is found in an appendix in the CRD. However, if the applicable CRD does not have a crosswalk, use the format shown in Table D-3.

c. **Step 3**. Build a DISR online standards profile (TV-1). See Enclosure L.

d **Step 4** Complete a LISI profile. (Interoperability Profile). These profiles are required prior to submitting the CPD. See Enclosure K.

e. **Step 5**. Include the NR-KPP statement. The NR-KPP definition statement will document that all requirements will be satisfied to the standards specified in the threshold and objective values.

KPP	**Threshold**	**Objective**
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture.	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture.

Table G-1. CPD NR-KPP Statement

* Information exchange processing is defined as: The input, output, verification, organization, storage, retrieval, transformation, and extraction of information from data.

f. **Step 6.** Include the Key Interface Profile (KIP) Implementation Statement. The statement expands on the declaration given in the CDD to include an explanation of how well the design complies with the KIPs. It includes the required KIP specification values and the corresponding system design values. The KIP statement alone does not ensure interoperability; a system must also be designed against the appropriate architectures, most current version of the DOD DISR and IA standards.

g. **Step 7.** Include an IA statement of compliance reading, " This system is currently in full compliance with DOD Directive 8500.1 and has made the required Information Assurance documentation available to the Joint Staff J-6 for review."

5. CPD Assessment Criteria. Table G-2 below provides criteria to assist assessors in reviewing a CPD in support of the J-6 Interoperability Requirements Certification.

No.	CPD Para	Criteria	Reference
1.		Does the CPD include top-level graphic(s) OV-2, OV-4, OV-5, and OV-6c?	CJCSI 6212.01C
2.		Does the CPD include top-level systems graphics-SV-1 (or SV-2 in the case of network systems), SV-4, SV-5, and SV-6?	CJCSI 6212.01C
3.		Does the CPD include a TV-1 generated by the DISR online standards profile tool?	CJCSI 6212.01C
4.		Do the architecture graphics include a short complete description that describes the architecture, its intended use, and discusses the top-level exchanges depicted in the view?	CJCSI 6212.01C
5.		Are the architecture graphics traceable between each view?	CJCSI 6212.01C
6.		Do the architecture graphics present a top-level view of the system's interoperability requirements with other current and known future systems? The focus of the graphic is to present a top-level view of the system's interoperability requirements with other current, and known future systems. Top-level is that level of detail required to graphically illustrate how the new system exchanges information between other combatant commanders, Services, agencies, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will show simple connectivity and can be annotated to show what information is exchanged.	CJCSI 6212.01C
7.		Do the CPD architecture graphics correlate with the associated CRD architecture graphics?	CJCSI 6212.01C
8.		Do the architecture mandatory views contain all mandatory fields in the required format?	CJCSI 6212.01C
9.		Does the CPD identify the top-level information exchanges for the system for each mission area that the system is proposed to support (e.g., CAS, AAW, surveillance, and reconnaissance)?	CJCSI 3170.01
10.		Do the CPD NR-KPP definitions include all appropriate elements of the associated CRD NR-KPP?	CJCSI 6212.01C
11.		Do the CPD system architecture views identify specific current and known IT and NSS sub-systems	CJCSI 6212.01C

No.	CPD Para	Criteria	Reference
		and interfaces that need to exchange information? The system interface description links together the operational and systems architecture views by depicting the assignments of subsystems and their interfaces to the systems and need lines described in the high level operational graphic diagram.	
12.		Does the CPD describe considerations for joint, combined, and coalition use?	CJCSI 3170.01
13.		Does the CPD identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO, and other allied and friendly nation systems?	CJCSI 3170.01
14.		Does the CPD require the system to comply with applicable information technology standards contained in the current DOD DISR?	CJCSI 6212.01
15.		If PKI is required, does the CPD include a statement that public key infrastructure (PKI) technology will be acquired as part of this effort and will be installed and used, including in initial fielding efforts, to ensure information security over all voice, video, and data transmission? PKI implementation should also consider communications interoperability with commercial and multinational partners.	CJCSI 3170.01
16.		Does the CPD address the interconnection of systems operating at different classification levels? What information assurance concepts does your program implement?	CJCSI 3170.01
17.		Does the CPD identify a requirement for spectrum supportability?	CJCSI 6212.01C
18.		Does the CPD address electromagnetic environmental effects (E3)?	CJCSI 6212.01C
19.		Does the CPD address host nation approval?	CJCSI 6212.01C
20.		Does the CPD identify unique user interface requirements, documentation needs, and special software certificates?	CJCSI 3170.01
21.		Does the CPD identify requirements for radio-based communications that will be satisfied by the joint tactical radio system (JTRS) CPD?	CJCSI 6212.01C
22.		Does the system identify requirements for data	CJCSI

No.	CPD Para	Criteria	Reference
		correctness, data availability and data processing ?	6212.01C
23.		Does the CPD include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the CPD clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment after 1 October 2002?	CJCSI 6212.01C
24.		Does the CPD adequately address the requirement for interoperability system testing and certification?	CJCSI 3170.01
25.		Does the CPD have a final TV-1 generated by DISR online?	CJCSI 6212.01C
26.		Does the CPD have a complete LISI interoperability requirements profile?	CJCSI 6212.01C
27.		Does the CPD contain a KIP Implementation Statement?	CJCSI 6212.01C
28.		Does the CPD identify applicable predecessor documents?	CJCSI 6212.01C

Table G-2. CPD -- J-6 Interoperability Certification and Assessment Criteria

6. Net Centric Assessment Criteria. Table G-3 below provides criteria to assist program managers to characterize the net-centric attributes of their services and data products. This characterization will assist Domain Managers to determine which programs should be transformed, sustained, or eliminated and to identify new starts.

Question	Description	Map to Checklist
General Information [establishes the general context of the system for analysis]		

Question		Description	Map to Checklist
1.	Which domain(s) is the program a member? If multiple domains, which is primary? Which capabilities does the program provide?	This should be one or more of the business or warfighting domains. **Warfighter** -- Battlespace Awareness; Command and Control; Force Application; Protection; Focused Logistics **Business** -- Logistics; Acquisition/Procurement; Finance, Accounting Operations, Programming, Budgeting and Funds Control; Real Property & Environmental Liabilities; Human Resources This should give an indication of the scope of program, e.g., Army payroll processing, weapons targeting, etc.	N/A
2.	What edge devices do the program support/or is programmed to support?	This identifies the minimum expected physical computing capabilities of the users, e.g., PDAs, radios, desktop computers, etc.	N/A
3.	What is current and projected subscriber population?	This would indicate anticipated/known user base, e.g., entire Department, Navy, single ship, 500 OSD personnel, federal and local agencies, commercial businesses, coalition/foreign nationals, etc.	N/A

Question		Description	Map to Checklist
4.	How does/will the program support weakly connected (e.g., "disadvantaged") users?	This looks for support to low bandwidth users or intermittently connected users, e.g., thin client applications, compression technologies, subscription services, etc.	N/A
Architecture			
5.	Which DOD integrated architecture is the program compliant?	DISR, DOD Arch. Framework**,** NCOW, COE, NMCI, other?	N/A
6.	Which of the NCOW RM emerging protocol standards does/will the program use?	The Net Centric Operations and Warfare – Reference Model (NCOW RM) Technical View-2 standards URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/index.htm	N/A
7.	Is the program IP-network enabled? Does it implement [programmed to] IPv4 and IPv6?	The policy is to implement IPv6, but to support IPv4 until IPv6 is implemented.	IP
Services			

Question		Description	Map to Checklist
8.	Which enterprise services in the NCOW RM, Operational View-5, does the program provide or is programmed to provide? How does the program provide [plan to] advertise the services? Schedule?	This would indicate the types of services that are provided, e.g., discovery service, mediation service, etc., which are becoming the standard as defined by the GIG ES Capabilities Development Document (CDD). URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/main.htm Addressing "how program provides services" should describe architecture, what technologies are being used (e.g., Web Services Definition Language [WSDL]), whether the service is registered and catalogued so it can be discovered by the Enterprise or other COIs, and whether service interfaces are defined.	Application diversity, OHIO
9.	What services in the NCOW RM does the program access [plan to access] that are provided by others? How does the program access [plan to access] the services? Schedule?	This should indicate what Core Enterprise Services or Domain or COI services program uses, e.g., NCES discovery service, C2 targeting service, etc., that are becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]. Addressing "how program access" should identify necessary interfaces, technologies.	Data centric

Question		Description	Map to Checklist
10.	What other services do the program provide [programmed to provide]? How does the program provide [plan to provide] the services? Schedule?	This would identify any other services that are being offered and the approach to implementing them, e.g., application services that are becoming the standard as defined by the GIG ES CDD.	Data centric, Application diversity
11.	To whom does the program offer [plan to offer] services (e.g., entire DOD Enterprise, subscribers' base, a COI?)	This indicates whether the program is developing services for its own exclusive use or as shareable services for others.	Apps on the Web
12.	Does the program have or plan to commit to a Service Level Agreement (SLA)?	This commits a program to delivering the level of service specified in the SLA and provides external users a level of expectation.	Quality of Service
13.	Will the program use the common service for Identification and Authorization?	To identify whether these functions are projected to be stove-piped and local to the program, common to the COI/Domain or provided by a common service.	Application diversity
Data Aspects			

Question		Description	Map to Checklist
14.	What data does the program generate and make available to the Enterprise or Communities of Interest? What processing does the program perform prior to posting the data? Is the program data a primary source or authoritative data?	Indicate which data assets (information products) will be shared with the Enterprise or within or outside program domain, e.g., databases, target tracks, UAV video feeds, etc. Also, indicate at what points in program data processing that the data will be made available, e.g., raw imagery, enhanced imagery, or enhanced imagery overlaid with troop locations. This indicates whether the data is the source or a copy of the primary source (duplicated).	OHIO, Post in parallel
15.	How does program advertise or plan to advertise its data (make it discoverable)? What is the plan to advertise in the future if the program is not using a registry today? When**?**	This indicates that discovery metadata is being generated for that data (compliant with DOD Discovery Metadata Spec that is becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]), the level of granularity for which discovery metadata is provided (e.g., metadata created for an entire database vs. individual records); the existence of a catalog, etc.	Data centric

Question		Description	Map to Checklist
16.	How does program make or plan to make that data available to other users?	This should address how the data will be made accessible to users on the network (e.g., storage accessible on the network, Web services that expose the application data). Must also indicate whether data access will be restricted based on security accesses. This should also describe the technique used to bind the requestor to the service (e.g., Web Services Definition Language [WSDL]).	Data centric, OHIO
17.	How does the program provide or plan to provide information about program data so that it can be accessed? If not using the DOD Metadata Registry and Clearing House, what is the plan to do so and when?	This would identify what metadata is being registered in the DOD Metadata Registry (main or federated registry), e.g., taxonomies, data dictionaries, schemas, etc	Data centric
18.	What percentage of the program's data is or will be available to other Domains/COIs?	This indicates the degree to which a program's data is accessible/shared.	Data centric, OHIO
Application			

Question		Description	Map to Checklist
19.	Is the system NCOW compliant? Is the system registered on the net for discovery? If not, what is the schedule?	Users can discover and use the system for data manipulation or collaboration.	Application diversity
IA/Security			
20.	What security domain does/will the program support?	Compartmented, SCI, TS, SECRET, and FOUO, Unclass?	N/A
21.	How does or will program authenticate the service requestor at the transport layer? How does/will program mediate security assertions (to pass security related information between systems, processes, and domains)? What architectural options are/will be used to provide "defense in depth" in the service-oriented architecture?	This would describe how the security context is extended from the request originator to the service application. This would define the method/standards being used to insert security assertions into the requesting message (e.g., Security Assertions Markup Language [SAML]) This would define whether XML gateways/firewalls are used, the use of Public Key Infrastructure (PKI), SAML-in-SOAP (Simple Object Access Protocol), or whether the service application itself is used to implement XML-signature, XML-encryption, etc.	Dynamic allocation of access

Question		Description	Map to Checklist
22.	What data does/will the program need to exchange across security domains (e.g., email, structured data sets, unstructured documents, imagery, etc.)? How does/will the program accomplish or plan to accomplish the exchange? Is this mechanism/capability inherent in the program or dependent upon some other program for this capability and if known, which program?	Indicate the type of data to be exchanged and its classifications and/or handling caveats. Indicate between which security domains it will be exchanged (one way/both ways) and type of cross-domain solution (e.g., guard) used.	Application diversity, Dynamic allocation of access
23.	If the program's IA/security services were not described in the Services section of this questionnaire, how does or will the program manage identity and privileges?	Indicate whether the product or service will confirm identity of users and processes through PKI certificates. Will the product or service be access-controlled or open to all users?	Dynamic allocation of access

Question		Description	Map to Checklist
24.	Is your program compliant with the IA component of the GIG Architecture?	This addresses whether a program is aware of the need to comply with the IA architecture component.	Dynamic allocation of access

Table G-2. CPD -- J-6 Interoperability Certification and Assessment Criteria

INTENTIONALLY BLANK

ENCLOSURE H

REQUIREMENTS GENERATION SYSTEM (RGS)

1. General. This enclosure provides guidance for assessing Operational Requirements Documents (ORDs). The Joint Staff will supersede this enclosure when all of the RGS documents have been exhausted from the system and JCIDS documents have been fully integrated.

2. Applicability. The enclosure applies to requirements documents submitted under the requirements generation system (CJCSI 3170.01C). This enclosure will be obsolete upon notification from the Joint Staff J-8.

3. Cancellation. The types of documents discussed in Enclosure H are expected to be absorbed into the new acquisition system, over the next 6 months. When the Joint Staff J-8 publishes a cancellation of the types of documents currently required by CJCSI 3170.01C, the policy and procedures in this enclosure are also canceled.

4. Top-Level Interoperability Information Exchange Requirements (IERs)

a. For ORDs, top-level IERS are defined as those information exchanges that are external to the system (i.e., with other combatant commands/Services/agencies (C/S/A), allied and coalition systems).

b. A top-level IER matrix provided in a worksheet format will be part of ORDs when submitted.Top-level IERs identify **who** exchanges **what** information with **whom, why** the information is necessary, and **how** the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission.

c. Top-level IERs and the interoperability KPP will be extracted from the ORD and used in the development of the C4ISP. Top-level IERs will be provided in the matrix format shown in Table D-1.

d. Top-level IERs may also be imported into modeling and evaluation including network warfare simulation (NETWARS) and Joint C4ISR architecture planning and analysis system (JCAPS). NETWARS and JCAPS both require additional fields than those depicted in Figure D-1.

e. Note that there is more detail in an ORD top-level IER matrix than in a CRD top-level IER matrix. The ORD will include all applicable top-

level IER(s) identified in the CRD (if a CRD exists). If the ORD is using a time-phased, evolutionary or block requirements approach, the ORD must identify the IERs for each phase or block.

f. The top-level IER matrix must correlate with the proposed high-level operational concept graphic(s) and system interface description.

(1) Sample ORD top-level IER matrices are illustrated in Table D-2.

(2) In the development of the top-level IER matrix, the originator will determine if a given top-level IER is critical (top-level IER matrix field 6).

g. An ORD critical top-level IER supports its associated CRD critical top-level IER, or will severely and adversely impact on a warfighter mission if not accomplished.

5. Interoperability Key Performance Parameter (I-KPP)

a. ORD interoperability KPPs, and hence the IERs that the interoperability KPPs are derived from, will be measurable and testable.

b. Top-level IERs will be used as the basis to develop interoperability KPPs. The I-KPP interoperability KPP definition will include that all top-level IERs will be satisfied to the standards specified in the threshold and objective values.

c. Typically the threshold criterion for the interoperability KPP will be 100 percent accomplishment of the critical top-level IERs, and the objective criterion for the interoperability KPP will be the accomplishment of all top-level IERs.

d. If a time-phased evolutionary or block approach to stating ORD requirements is being used, the ORD should identify a separate Interoperability KPP for each phase or block.

6. Assessment Criteria Checklists

a. The Appendices to Enclosure H contain checklists of assessment criteria to be used when reviewing Operations Requirements Documents for J-6 Interoperability Certification.

b. Appendix A to Enclosure H contains the checklist for ORDs.

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE H

OPERATIONAL REQUIREMENTS DOCUMENT (ORD)

1. General. This appendix includes the interoperability assessment requirements for an ORD, which terminate 24 December 2003.

2. Applicability. The checklist shown immediately below applies to all ORDs submitted under the Requirements Generation System

Table H-A-1 ORD ASSESSMENT CRITERIA

No	ORD Para	Criteria	Reference
1.	1	Does the ORD describe the C4ISR (information exchange) operational concept?	CJCSI 3170.01C
2.	1	For ORDs without MNSs only: Does the ORD describe how the requirement relates to the OSD PSAs, DOD Chief Information Officers, and DOD component strategic planning?	CJCSI 3170.01C
3.	1	For ORDs without MNSs only: Does the ORD describe the functional area or activity's current organization and operational environment and describe the shortfalls of existing capabilities?	CJCSI 3170.01C
4.	1	For ORDs without MNSs only: Does the ORD describe quantitative benchmarks of process performance in terms of speed, productivity, and quality of outputs where comparable processes exist in the public or private sectors?	CJCSI 3170.01C
5.	2	Does the ORD summarize the threat to be countered and projected threat environment (NOTE: Should reference DIA- or service technical intelligence center-approved documents)?	CJCSI 3170.01C
6.	3	Does the ORD describe why existing C4ISR operational, system, and technical architecture views cannot meet the requirements for the proposed system?	CJCSI 3170.01C
7.	4	Does the ORD contain a high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
8.	4	Does the high-level operational graphic(s) (OV-1) present a top-level view of the system's interoperability requirements with other current and known	CJCSI 3170.01C

No	ORD Para	Criteria	Reference
		future systems? The focus of the graphic is to present a top-level view of the system's interoperability requirements with other current, and known future systems. Top-level is that level of detail required to graphically illustrating how the new system exchanges information between other C/S/A, allied, and coalition systems. The graphic will show such things as missions, top-level operations, organizations, and geographical distribution of assets. The lines connecting the systems will show simple connectivity and can be annotated to show what information is exchanged.	
9.	4	Does the ORD high-level operational graphic(s) (OV-1) correlate with the associated CRD high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
10.	4	Does the ORD contain a system interface description (SV-1)?	CJCSI 3170.01C
11.	4	Does the ORD system interface description (SV-1) identify specific current and known IT and NSS sub-systems and interfaces that need to exchange information? The system interface description links together the operational and systems architecture views by depicting the assignments of subsystems and their interfaces to the systems and needlines described in the high level operational graphic diagram.	CJCSI 3170.01C
12.	4	Does the ORD system interface description (SV-1) correlate with the provided ORD high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
13.	4	Was a top-level IER matrix (OV-3) provided in a worksheet format?	CJCSI 3170.01C
14.	4	Does the ORD top level IER matrix (OV-3) contain all mandatory fields in the required format?	CJCSI 3170.01C
15.	4	Does the ORD identify the top-level IERs for the system for each mission area that the system is proposed to support (e.g., CAS, AAW, surveillance, and reconnaissance)?	CJCSI 3170.01C
16.	4	Does the ORD top-level IER matrix (OV-3) identify **who** exchanges what information with **whom**, **why** the information is necessary, and **how** the information exchange must occur? Top-level IERs identify the elements of warfighter information used in support of a particular mission-related task and	CJCSI 3170.01C

No	ORD Para	Criteria	Reference
		exchanged between at least two operational systems supporting a joint mission area.	
17.	4	Are all ORD top-level IERs designated critical if they are required to support an associated CRD critical top-level IER or will severely and adversely impact on a warfighter mission if not accomplished?	CJCSI 3170.01C
18.	4	Does the ORD top-level IER matrix (OV-3) correlate with all applicable top-level IERs in the associated CRD top-level IER matrix?	CJCSI 3170.01C
19.	4	Does the ORD top level IER matrix correlate with the associated ORD system interface description and ORD high-level operational graphic(s) (OV-1)?	CJCSI 3170.01C
20.	4	Does the ORD I-KPP definition include that all top-level IERs will be satisfied IAW their critical code to the standards specified in the threshold and objective values?	CJCSI 3170.01C
21.	4	Do the ORD I-KPP threshold criteria include 100 percent accomplishment of the critical top-level IERs?	CJCSI 3170.01C
22.	4	Do the ORD I-KPP objective criteria include 100 percent accomplishment of the critical top-level IERs and of most or all non-critical top-level IERs?	CJCSI 3170.01C
23.	4	Do the ORD I-KPP definitions include all appropriate elements of the associated CRD NR-KPP?	CJCSI 3170.01C
24.	4	Are the ORD I-KPPs measurable and testable?	CJCSI 3170.01C
25.	4	Does the ORD address natural and man-made environmental factors (such as electromagnetic compatibility and acoustic or atmospheric propagation constraints)?	CJCSI 3170.01C
26.	4	Does the ORD address safety issues' regarding hazards of electromagnetic radiation to ordnance (HERO)?	CJCSI 3170.01C
27.	4	Does the ORD identify physical and operational information system security needs?	CJCSI 3170.01C
28.	5	Does the ORD establish information systems support objectives for initial and full operational capabilities? NOTE: Must discuss interfacing IT and NSS at the system, subsystem, platform, and force levels. Should focus on support objectives related to IT and NSS standardization and interoperability.	CJCSI 3170.01C
29.	5	Does the ORD describe how the system will be	CJCSI

No	ORD Para	Criteria	Reference
		integrated into the IT and NSS architecture that is forecast to exist when the system is fielded?	3170.01C
30.	5	Does the ORD identify data and data fusion requirements (data, voice, video), computer network support, and anti-jam requirements?	CJCSI 3170.01C
31.	5	Does the ORD identify unique intelligence information requirements, including intelligence interfaces, communications, and database support pertaining to the target and mission planning activities, threat data, etc?	CJCSI 3170.01C
32.	5	Does the ORD describe considerations for joint, combined, and coalition use?	CJCSI 3170.01
33.	5	Does the ORD identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO, and other allied and friendly nation systems?	CJCSI 3170.01C
34.	5	Does the ORD require the system to comply with applicable information technology standards contained in the current DOD DISR?	CJCSI 3170.01C
35.	5	Does the ORD address interface requirements with the Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Defense Message System (DMS), Global Command and Control System (GCCS), or the Common Operational Picture (COP)?	CJCSI 3170.01C
36.	5a	Is the requirement for an adequate level of IA required for all DOD systems that are used to enter, process, store, display, or transmit DOD information, regardless of classification or sensitivity addressed in the ORD?	CJCSI 3170.01C
37.	5	As part of the IA solution, does the ORD include a statement that public key infrastructure (PKI) technology will be acquired as part of this effort and will be installed and used, including in initial fielding efforts, to ensure information security over all voice, video, and data transmission? PKI implementation should also consider communications interoperability with commercial and multinational partners.	CJCSI 3170.01C
38.	5	Does the ORD address the interconnection of systems operating at different classification levels?	CJCSI 3170.01C
39.	5	Does the ORD address E3?	CJCSI

No	ORD Para	Criteria	Reference
			3170.01C
40.	5	Does the ORD identify a requirement for spectrum supportability?	CJCSI 3170.01C
41.	5	Does the ORD identify a requirement to obtain host-nation approval (HNA) for equipment intended for operation in an overseas area of operations?	CJCSI 3170.01C
42.	5	Does the ORD identify computer resource constraints (examples include language, computer, database, architecture, or interoperability constraints)?	CJCSI 3170.01C
43.	5	Does the ORD address all mission critical and support computer resources, including automated test equipment?	CJCSI 3170.01C
44.	5	Does the ORD identify unique user interface requirements, documentation needs, and special software certificates?	CJCSI 3170.01C
45.	5	Does the ORD identify cartographic materials, digital geospatial data, and geodetic data needed for system employment? NOTE: Where possible, NIMA standard data and DOD formats will be used.	CJCSI 3170.01C
46.	5	Does the ORD identify requirements for radio-based communications that will be satisfied by the joint tactical radio system (JTRS) ORD?	CJCSI 3170.01C
47.	5	Does the ORD include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the ORD clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment after 1 October 2002?	CJCSI 3170.01C
48.	7	Does the ORD include the number of operational systems, operational and support personnel, facilities, support infrastructure and organizational, intermediate, and depot support elements that must be in place? NOTE: The impact of not meeting this objective and a window of acceptability must be addressed.	CJCSI 3170.01C
49.	7	Does the ORD adequately address the requirement for interoperability system testing and certification?	CJCSI 3170.01C

(INTENTIONALLY BLANK)

ENCLOSURE I

INFORMATION SUPPORT PLANS (ISP)

1. General

a. All systems – Acquisition Category (ACAT), non-ACAT, and fielded systems – must be evaluated and certified prior to (initial or updated) fielding, and periodically during their entire life (see reference g). The Information Support Plan (ISP) addresses all ACAT, non-ACAT, and fielded systems. The program authority shall prepare an ISP to document the IT and NSS needs, objectives, interface requirements for all non-ACAT and fielded programs. The Interoperability Requirements Certification process for an ISP is shown in Figure I-1.

b. The ISP will contain sufficient detail (commensurate with the size of the program/effort) to permit an evaluation of the associated interoperability and supportability requirements. Depending on the scope, size, and impact of the system, the Joint Staff may recommend that the ISP transition to a JCIDS document.

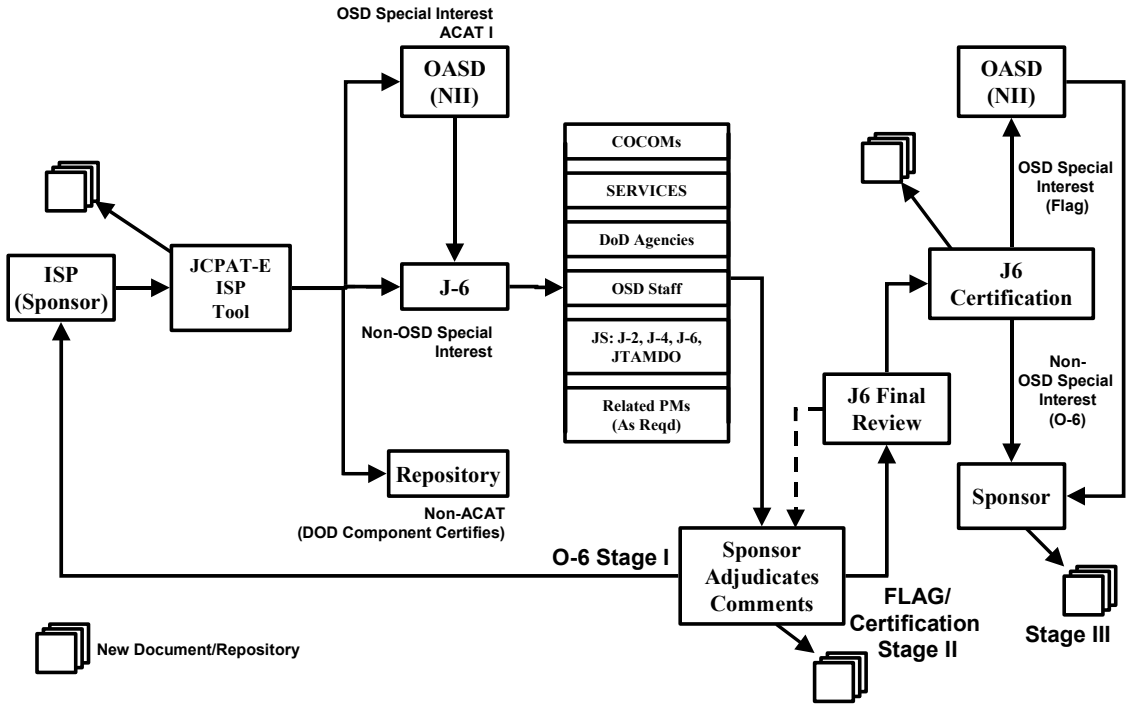

Figure I-1. ISP Interoperability Requirements Certification

2. Applicability. This enclosure applies to all ACAT, non-ACAT and fielded programs regardless of approval authority, designation, increment, or block.

3. Net-Ready Key Performance Parameter. All ISPs for systems that exchange information with other systems will contain a Net-Ready KPP. For all ISPs with an associated approved JCIDS CDD or CPD capabilities document, the ISP can refer to the associated CDD/CPD. ISPs for CRDs, ORDs, non-ACAT and fielded systems will include the NR-KPP in the ISP. The NR-KPP will consist of the following:

a. AV-1, OV-2, OV-4, OV-5, OV-6C

b. SV-4, SV-5, SV-6

c. TV-1 generated from DISR online

d. Applicable CRD crosswalk (See Table D-3)

e. Initial LISI Profile (Interface Requirements Profile) See Enclosure K

f. NR-KPP statement. (Table I-1)

g. IA Statement of Compliance

h. Key Interface Profile (KIP) Declaration (list of the KIPS that apply to the system)

4. NR-KPP defines interoperability for the proposed system. The NR-KPP will be derived from all of the activity interfaces, services, policy-enforcement controls, data-sharing of the NCOW-RM, GIG-KIPs, the specific Joint integrated architecture products (including data correctness, data availability and data processing), and information assurance accreditation requirements. PMs will comply with the applicable KIPs to the maximum extent practicable as they become available.

5. ISPs that come under the umbrella of a CRD must ensure compliance with the CRD NR-KPP (Enclosure D) for those capabilities common to both the ISP and the CRD.

6. Migration to the Net-Ready Key Performance Parameter (NR-KPP). Just as was done with CJCSI 3170 regarding top down architectures, it is recognized that all the KIPs are not available, but the process must be put in motion for future system development.

a. Figure I-2 below depicts the migration timeline to the NR-KPP.

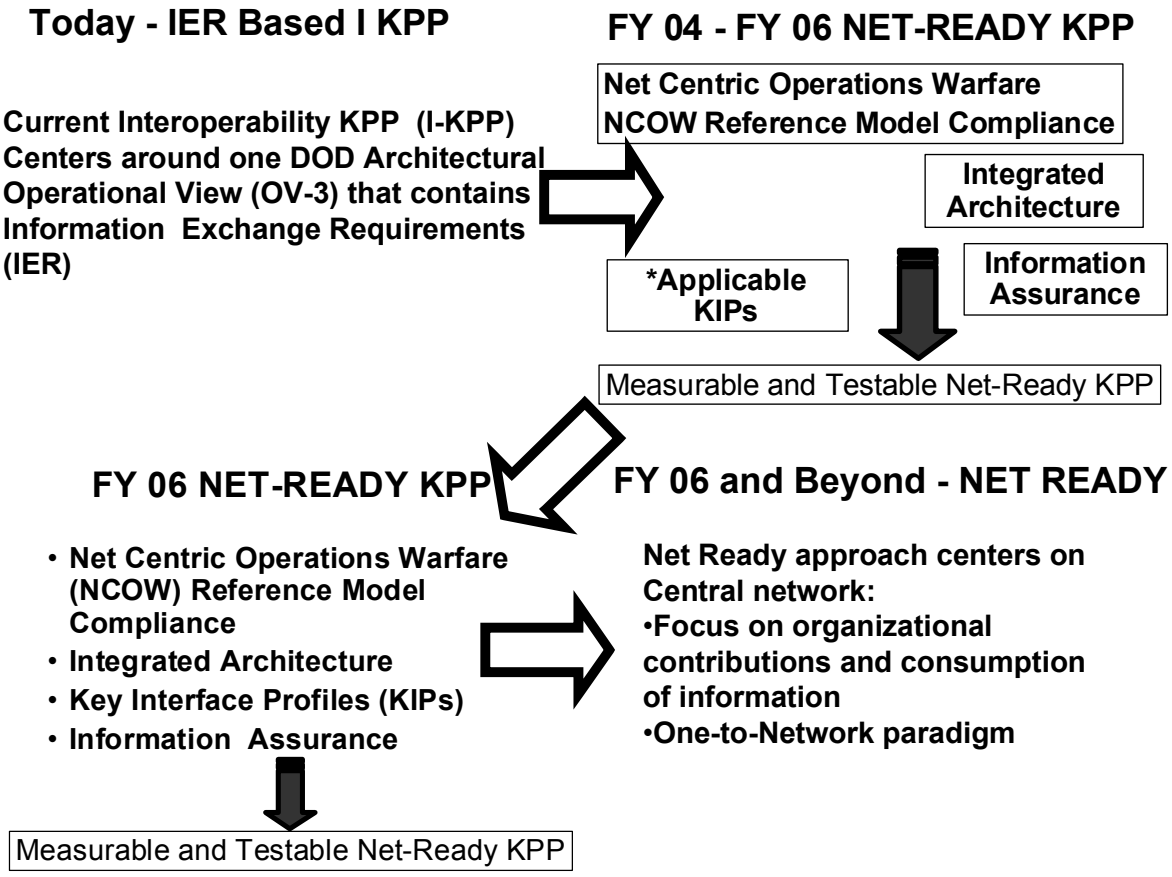

Figure I-2. Migration to the Net-Ready KPP

b. FY 04 to FY06. Program managers will comply with three parts of the NR-KPP:

(1) Architectures products. See Table A-2. PMs producing the Architectures Products, using the NCOW, should to develop high-level interface information for becoming Net Ready and also be Key Interface tolerant to adapt to the Key Interface Profiles as they are profiled and become available.

(2) Net-Centric Operations Warfare (NCOW) Reference Model. NCOW RM provides the PM with a common lexicon for NCOW concepts and terminology, supported by recognizable architectural descriptions. It describes net-centricity at the enterprise level for DOD Program Managers and other decision makers. It includes Overview and Summary Information (AV-1), Integrated Dictionary (AV-2), High-level Operational Concept Graphic (OV-1), Activity Model (OV-5), and Target Technical View.

(3) Information assurance. For PMs, for each lifecycle development activity, IAW DOD Directive 5000.1 (reference d), there is a corresponding set of security activities that shall verify compliance with the security requirements and evaluate vulnerabilities.

(4) As Key Interfaces which have been profiled and made available through the DOD IT Standards Repository (DISR). PMs will comply with these KIPs, which will be published as an annex in DOD IT Standards Repository (DISR). KIP's will be distributed as an advisory as soon as they have been defined, and will be formally published on a priority basis. PM's are required to incorporate published KIPs in all new start or significantly modified systems acquisitions and/or pre-Milestone B designs immediately. For ongoing acquisitions beyond Milestone B and/or established systems, published KIPs will included as objective capabilities immediately, and as threshold requirements within 12 months of publication through the systems evolutionary spiral block upgrade process.

(5) FY 06 and beyond. PMs will be expected to comply with all parts of the Net Ready Key Performance Parameter.

7. NR-KPP Development. Development of the NR-KPP begins with designing the architecture for the proposed system. Without an architecture the systems will not meet its goals nor meet any interoperability requirements. Each architecture view has a purpose and can be traced back to the operational concept.

a. **Step 1**. Develop the mandatory architecture views.

(1) The format and description for all of the architectural views will be IAW with the most current version of the DOD Architecture Framework (reference n). All of the fields/columns for each architecture view from reference n are mandatory.

(2) A short description of the view, its intended use and a discussion of the top-level exchanges will accompany each view. The narrative for each view should be as concise as possible while still giving the necessary explanation of the view. A length of ½ page or less is ideal; some views may require a longer narrative.

b. **Step 2.** Complete the CRD Crosswalk. The format for the crosswalk for a particular CRD is found in an appendix in the applicable

CRD. However, if the applicable CRD does not have a crosswalk, use the format shown in Table D-3.

c. **Step 3**. Build a DISR online standards profile. This profile is required prior to submitting the ISP. See Enclosure L.

d. **Step 4.** Complete a LISI interoperability requirements profile. This profile is required prior to submitting the ISP. See Enclosure K.

e. **Step 5**. Include the NR-KPP statement. The NR-KPP definition statement will document that all requirements will be satisfied to the standards specified in the threshold and objective values. See Table I-1 below.

NR-KPP	**Threshold**	**Objective**
All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation specified in the threshold (T) and objective (O) values.	100 percent of interfaces, services, policy-enforcement controls, data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture.	100 percent of interfaces, services, policy-enforcement controls, data correctness, availability and processing* requirements in the Joint integrated architecture.

Table I-1. ISP NR-KPP Statement

* Data processing is defined as: The input, output, verification, organization, storage, retrieval, transformation, and extraction of information from data.

f. **Step 6.** Include the Key Interface Profile (KIP) Implementation Statement. The statement expands on the declaration given in the CDD to include an explanation of how well the design complies with the KIPs. It includes the required KIP specification values and the corresponding system design values. The KIP statement alone does not ensure interoperability; a system must also be designed against the appropriate architectures, most current version of the DISR and IA standards.

g. **Step 7.** Complete an IA compliance statement.

8. ISP Assessment Criteria. Table I-2 below provides criteria to assist assessors in reviewing ISP in support of the J-6 Interoperability Requirements Certification.

No	ISP Chapter	Criteria	Reference
1.	NA	Does this ISP have an associated JCIDS approved CDD/CPD? (for ACAT/JCIDS Programs)	6212.01C
2.	NA	Has the system been registered in JCPAT-E?	6212.01C
3.	NA	Has an IT standards profile been created in JCPAT-E?	6212.01C
4.	NA	Has an interoperability and interconnectivity profile been created in JCPAT-E?	6212.01C
5.	Ch 2	Have the warfighting missions or (functional domains for AIS programs) been identified?	DODI 4630.8
6.	Ch 2	Have information needs been identified for each warfighting mission or business domain?	DODI 4630.8
7.	Ch 2	Has a hierarchical functional capability diagram OV-5 (or equivalent) been provided that shows the supporting C4 systems (e.g. networks, radios, functional C2 systems etc.) necessary to achieve the desired operational or functional capabilities of the system?	DODI 4630.8
8.	Ch 2	Has an OV-2 (or multiple OV-2s) that identifies the operational nodes and elements that determine the communications needed been provided?	DODI 4630.8
9.	Ch 2	Have operational nodes been examined to determine internal information drivers (e.g. operational cells within a warfighting platform)?	DODI 4630.8
10.	Ch 2	Have quality criteria for the information needs that have been identified been provided?	DODI 4630.8
11.	Ch 2	If timeliness criteria exist, have they been identified?	DODI 4630.8
12.	Ch 2	Have quality criteria for the information needs that have been identified been provided?	DODI 4630.8
13.	Ch 2	Has method for transporting information been provided?	DODI 4630.8
14.	Ch 2	Have information quantities been established?	DODI 4630.8
15.	Ch 2	Has method for transporting information been provided?	DODI 4630.8
16.	Ch 2	Have supporting data repositories and access to them been identified?	DODI 4630.8

No	ISP Chapter	Criteria	Reference
17.	Ch 2	Have methods for information search or discovery been identified?	DODI 4630.8
18.	Ch 2	Has ability of transport systems to support the information needs been assessed?	DODI 4630.8
19.	Ch 2	Have systems connecting to JWICS or other SCI systems followed DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999 and DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 18 November 2002.	DODI 4630.8
20.	Ch 2	Has the synchronization of supporting programs been assessed?	DODI 4630.8
21.	Ch 2	Has requirement for spectrum supportability and a status of Spectrum Certification process been provided?	DODI 4630.8
22.	Ch 2	Is an analysis of compliance with the emerging Net-Centric Enterprise Services (NCES) / Core Enterprise Services (CES) provided?	DODI 4630.8
23.	Ch 2	Does the ISP identify requirements for radio-based communications that will be satisfied by use of software compliant radios in accordance with the Joint Tactical Radio System (JTRS) ORD?	DODI 4630.8
24.	Ch 2	Internet Protocol Version 6.0 (IPv6)?	DODI 4630.8
25.	Ch 2	Has the program's inconsistencies with the GIG Integrated Architecture been assessed and a plan for getting into alignment provided?	DODI 4630.8
26.	Ch 2	DOD Net-Centric Data Strategy?	DODI 4630.8
		For all ISPs without an associated approved JCIDS CDD or CPD capabilities document, the following items will be developed and included in the CDD and CPDs.	
27.	App	Does the ISP address electromagnetic environmental effects (E3)?	DODI 4630.8
28.	App	Does the ISP include a requirement for NAVSTAR global positioning system (GPS) and precise positioning service (PPS)? If yes, does the ISP clearly state that the system will develop and procure only selective availability anti-spoofing module (SAASM) based equipment after 1 October 2002?	CJCSI 6212.01C
29.	App	Does the ISP adequately address the requirement for interoperability system testing and	CJCSI 6212.01C

No	ISP Chapter	Criteria	Reference
		certification?	
30.	App	Does the ISP identify procedural and technical interfaces, communications, protocols, and standards required to be incorporated to ensure compatibility and interoperability with other Service, joint Service, NATO and other allied and friendly nation systems?	CJCSI 6212.01C
31.	App	Does the ISP describe considerations for joint, combined, and coalition use?	CJCSI 6212.01C
32.	App	Do the ISP NR-KPP definitions include all appropriate elements of the associated CRD NR-KPP?	CJCSI 6212.01C
33.	App	Do the ISP contain a complete NR-KPP adequately addressing the four essential elements of the NR-KPP (NCOW Reference Model, complete integrated architecture, information assurance and adherence to applicable defined Key Interface Profiles (KIPs))?	CJCSI 6212.01C

Table I-2. ISP – J-6 Interoperability and Supportability Assessment Criteria

Question	Description	Map to Checklist
General Information [establishes the general context of the system for analysis]		

Question		Description	Map to Checklist
1.	Which domain(s) is the program a member? If multiple domains, which is primary? Which capabilities does the program provide?	This should be one or more of the business or warfighting domains. **Warfighter** – Battlespace Awareness; Command and Control; Force Application; Protection; Focused Logistics **Business** – Logistics; Acquisition/Procurement; Finance, Accounting Operations, Programming, Budgeting and Funds Control; Real Property & Environmental Liabilities; Human Resources This should give an indication of the scope of program, e.g., Army payroll processing, weapons targeting, etc.	N/A
2.	What edge devices do the program support/or is programmed to support?	This identifies the minimum expected physical computing capabilities of the users, e.g., PDAs, radios, desktop computers, etc.	N/A
3.	What is current and projected subscriber population?	This would indicate anticipated/known user base, e.g., entire Department, Navy, single ship, 500 OSD personnel, federal and local agencies, commercial businesses, coalition/foreign nationals, etc.	N/A

Question		Description	Map to Checklist
4.	How does/will the program support weakly connected (e.g., "disadvantaged") users?	This looks for support to low bandwidth users or intermittently connected users, e.g., thin client applications, compression technologies, subscription services, etc.	N/A
Architecture			
5.	Which DOD integrated architecture is the program compliant?	DISR, DOD Arch. Framework**,** NCOW, COE, NMCI, other?	N/A
6.	Which of the NCOW RM emerging protocol standards does/will the program use?	The Net Centric Operations and Warfare – Reference Model (NCOW RM) Technical View-2 standards URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/index.htm	N/A
7.	Is the program IP-network enabled? Does it implement [programmed to] IPv4 and IPv6?	The policy is to implement IPv6, but to support IPv4 until IPv6 is implemented.	IP
Services			

Question		Description	Map to Checklist
8.	Which enterprise services in the NCOW RM, Operational View-5, does the program provide or is programmed to provide? How does the program provide [plan to] advertise the services? Schedule?	This would indicate the types of services that are provided, e.g., discovery service, mediation service, etc., which are becoming the standard as defined by the GIG ES Capabilities Development Document (CDD). URL: https://cao.hanscom.af.mil/af-cio/NCOW_ver0pt9/main.htm Addressing "how program provides services" should describe architecture, what technologies are being used (e.g., Web Services Definition Language [WSDL]), whether the service is registered and catalogued so it can be discovered by the Enterprise or other COIs, and whether service interfaces are defined.	Application diversity, OHIO
9.	What services in the NCOW RM does the program access [plan to access] that are provided by others? How does the program access [plan to access] the services? Schedule?	This should indicate what Core Enterprise Services or Domain or COI services program uses, e.g., NCES discovery service, C2 targeting service, etc., that are becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]. Addressing "how program access" should identify necessary interfaces, technologies.	Data centric

Question		Description	Map to Checklist
10.	What other services do the program provide [programmed to provide]? How does the program provide [plan to provide] the services? Schedule?	This would identify any other services that are being offered and the approach to implementing them, e.g., application services that are becoming the standard as defined by the GIG ES CDD.	Data centric, Application diversity
11.	To whom does the program offer [plan to offer] services (e.g., entire DOD Enterprise, subscribers' base, a COI?)	This indicates whether the program is developing services for its own exclusive use or as shareable services for others.	Apps on the Web
12.	Does the program have or plans to commit to a Service Level Agreement (SLA)?	This commits a program to delivering the level of service specified in the SLA and provides external users a level of expectation.	QoS
13.	Will the program use the common service for Identification and Authorization?	To identify whether these functions are projected to be stove-piped and local to the program, common to the COI/Domain or provided by a common service.	Application diversity
Data Aspects			

Question		Description	Map to Checklist
14.	What data does the program generate and make available to the Enterprise or Communities of Interest? What processing does the program perform prior to posting the data? Is the program data a primary source or authoritative data?	Indicate which data assets (information products) will be shared with the Enterprise or within or outside program domain, e.g., databases, target tracks, UAV video feeds, etc. Also, indicate at what points in program data processing that the data will be made available, e.g., raw imagery, enhanced imagery, or enhanced imagery overlaid with troop locations. This indicates whether the data is the source or a copy of the primary source (duplicated).	OHIO, Post in parallel
15.	How does program advertise or plan to advertise its data (make it discoverable)? What is the plan to advertise in the future if the program is not using a registry today? When**?**	This indicates that discovery metadata is being generated for that data (compliant with DOD Discovery Metadata Spec that is becoming the standard as defined by the GIG ES Capabilities Development Document [CDD]), the level of granularity for which discovery metadata is provided (e.g., metadata created for an entire database vs. individual records); the existence of a catalog, etc.	Data centric

Question		Description	Map to Checklist
16.	How does program make or plan to make that data available to other users?	This should address how the data will be made accessible to users on the network (e.g., storage accessible on the network, Web services that expose the application data). Must also indicate whether data access will be restricted based on security accesses. This should also describe the technique used to bind the requestor to the service (e.g., Web Services Definition Language [WSDL]).	Data centric, OHIO
17.	How does the program provide or plan to provide information about program data so that it can be accessed? If not using the DOD Metadata Registry and Clearing House, what is the plan to do so and when?	This would identify what metadata is being registered in the DOD Metadata Registry (main or federated registry), e.g., taxonomies, data dictionaries, schemas, etc	Data centric
18.	What percentage of the program's data is or will be available to other Domains/COIs?	This indicates the degree to which a program's data is accessible/shared.	Data centric, OHIO
Application			

Question		Description	Map to Checklist
19.	Is the system NCOW compliant? Is the system registered on the net for discovery? If not, what is the schedule?	Users can discover and use the system for data manipulation or collaboration.	Application diversity
IA/Security			
20.	What security domain does/will the program support?	Compartmented, SCI, TS, SECRET, and FOUO, Unclass?	N/A
21.	How does or will program authenticate the service requestor at the transport layer? How does/will program mediate security assertions (to pass security related information between systems, processes, and domains)? What architectural options are/will be used to provide "defense in depth" in the service-oriented architecture?	This would describe how the security context is extended from the request originator to the service application. This would define the method/standards being used to insert security assertions into the requesting message (e.g., Security Assertions Markup Language [SAML]) This would define whether XML gateways/firewalls are used, the use of Public Key Infrastructure (PKI), SAML-in-SOAP (Simple Object Access Protocol), or whether the service application itself is used to implement XML-signature, XML-encryption, etc.	Dynamic allocation of access

Question		Description	Map to Checklist
22.	What data does/will the program need to exchange across security domains (e.g., email, structured data sets, unstructured documents, imagery, etc.)? How does/will the program accomplish or plan to accomplish the exchange? Is this mechanism/capabil-ity inherent in the program or dependent upon some other program for this capability and if known, which program?	Indicate the type of data to be exchanged and its classifications and/or handling caveats. Indicate between which security domains it will be exchanged (one way/both ways) and type of cross-domain solution (e.g. guard) used.	Application diversity, Dynamic allocation of access
23.	If the program's IA/security services were not described in the Services section of this questionnaire, how does or will the program manage identity and privileges?	Indicate whether the product or service will confirm identity of users and processes through PKI certificates. Will the product or service be access-controlled or open to all users?	Dynamic allocation of access

Question		Description	Map to Checklist
24.	Is your program compliant with the IA component of the GIG Architecture?	This addresses whether a program is aware of the need to comply with the IA architecture component.	Dynamic allocation of access

Table I-3. Net Centric Assessment Criteria

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE I

INFORMATION SUPPORT PLAN FORMAT

1. The Information Support Plan (ISP) format in this enclosure will be replaced with the format in Enclosure 4 to reference g once reference g is issued.

2. Format. ISPs will contain an Introduction (consisting of an overview and program data); an Analysis Chapter that consists of an incremental analysis process that shall be appropriately tailored to each program; an Issues Chapter that details the information, interoperability and synchronization issues identified in the analysis section and the strategy to address or mitigate these issues. ISPs shall also include the following mandatory appendices: References, Systems Data Exchange Matrix (SV-6), Interface Control Agreements, and acronym list (AV-2). Other Appendices may be included, as necessary. The format within each chapter of an ISP may be tailored to include only those elements that apply to the subject program. DODI 4630.8 and the DOD 5000 Defense Acquisition Guidebook provide additional information for completing each chapter and appendix in the ISP.

a. Chapter 1 - Introduction. The introductory chapter shall be organized into two sections, overview and program data. Further details for overview and program data content are provided in the DOD 5000 Defense Acquisition Guidebook.

(1) Overview. Provides a brief introduction describing the scope of the program, the program's relationship to other programs, and the program's relationships to relevant JOC(s) and/or JFC(s), JCIDS documents and associated integrated architectures impacting the program. Do not duplicate JCIDS documentation content, but reference it as appropriate.

(2) Program Data. Provides background information to the ISP reviewer so that the reviewer can understand the context of the ISP. It also documents the status of the acquisition at the point in time that the ISP was developed.

b. Chapter 2 - Analysis. Supporting integrated architecture products shall be used in the ISP analysis (see Table I-A-1). It is not intended that the prescribed supporting integrated architecture products be developed for ISP purposes only, but rather that the ISP shall exploit existing

products to enable better understanding of required information needs for a given program or capability. Analysis of the sufficiency of IT and NSS information support needs shall be accomplished in terms of the operational and functional capabilities that are being supported. This analysis requires an understanding of the operational and functional capabilities, and associated metrics to assess and evaluate: organizations; organizational relationships; operational activities; node connectivity and required system data exchanges required to achieve a given capability. Table I-A-1 lists the steps in the ISP information needs discovery and analysis process. Further details on accomplishing these steps are provided in the DOD 5000 Defense Acquisition Guidebook.

Step 1: Identify the warfighting missions (or functions within the enterprise business domains).
Step 2: Identify information needed to support operational/functional capabilities for each warfighting mission identified in step 1.
Step 3: Determine the operational users and notional suppliers of the information needed.
Step 4: Establish the quality of the data needed to support the functions identified in the programs integrated architecture.
Step 5: Determine if timeliness criteria exist for the information.
Step 6: Determine/Estimate the quantity of information of each type that is needed.
Step 7: Discuss how the information will be accessed or discovered.
Step 8: Assess the ability of supporting systems to supply the necessary information.
Step 9: Discuss RF Spectrum needs.
Step 10: Perform a Net Centric Assessment.
Step 11: Discuss the program's inconsistencies with the GIG Integrated Architecture and its strategy for getting into alignment.
Step 12: Discuss the program's Information Assurance strategy and reference the Program Protection Plan.
Step 13: Identify Information support needs to support development, testing and training.

Table I-A-1. Information Needs Discovery and Analysis Process

c. Chapter 3 - Issues. Issues shall be presented in a table (see Table I-A-2) or an outline containing the same data. Operational issues shall be grouped under the mission impacted, then under the functional capability impacted under that mission. When an issue involves more than one mission, subsequent missions shall be marked with the previous issue number and those fields that are the same as the original, should be marked as such. If the issue's impact differs between missions, then the description for each mission may also differ accordingly. The following minimum column headings: Issue Number; Supporting System; Issue, Issue Description; Issue Impact; and Mitigation Strategy or Resolution Path). Number each issue as "C-#" for critical shortfalls and "S-#" for substantive issue. Issues shall include resolution paths with projected dates to be corrected. If resolution details are not known, a discussion on the approach (including anticipated responsible parties) shall be provided.

Operational Issues					
Mission					
Functional Capabilities impacted					
Issue number	**Supporting system**	**Issue**	**Issue Description**	**Issue Impact**	**Mitigation Strategy/Resolution Path (and Time-Frame)**
Development Issues					
Testing Issues					
Training Issues					

Table I-A-2. Issue Summary

d. Appendices

(1) Appendix A -- References. Identify all related documents (with dates) used to prepare the ISP. All essential and supporting products used in the ISP analysis shall be listed in Appendix A, to include: integrated architecture products; the System Threat Assessment; Analysis of Alternatives; JCIDS documentation; TEMP; System Acquisition Master Plan (SAMP); Acquisition Strategy; Acquisition Program Baseline (APB); and ISPs for other systems. Except for the approved or draft JCIDS documents, do not include copies of the reference documents. Indicate sources for any documents that are not available electronically from the program office.

(2) Appendix B. -- Systems Data Exchange Matrix (SV-6). Appendix B will consist of a detailed SV-6 matrix derived from the associated integrated architectures, with narrative discussion as necessary. Provide additional systems data exchange information (and supporting discussion), identified during the ISP analysis, for each system interface, if not already incorporated in JCIDS documentation. These will be discussed in the main body of the ISP in the Analysis Section.

(3) Appendix C. -- Interface Control Agreements. Identify documentation that indicates agreements made (and those required) between the subject ISP program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

(4) Appendix D. -- Acronym List. Provide an Integrated Dictionary formatted as an AV-2.

(5) Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant JCIDS documents. Additional, or more detailed information, used to satisfy DOD component-specific requirements, shall be included as an appendix, and not incorporated in the body of the subject ISP. Additional architecture views used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP. NOTE: For all ISPs without an associated approved JCIDS CDD or CPD capabilities document, the following items will be developed and included

in the appendices (these are already developed and included in the CDD and CPDs):

a. NR-KPP

b. Statement addressing compliance with:

(1) JTRS ORD (for radio systems)

(2) Electromagnetic environmental effects and spectrum supportability

(3) Host Nation Approval (HNA)

(4) NAVSTAR Global Positioning System (GPS) and Precise Positioning Service (PPS) and that the system will develop and procure only Selective Availability Anti-Spoofing Module (SAASM) based equipment

(5) Other items identified in the checklist at Table I-2

c. CRD Crosswalk for all applicable CRDs

d. System Registration in JCPAT-E IAW Enclosure J

e. Interoperability and Interconnectivity Profile (IIP) using JCPAT-E IAW Enclosure K

f. IT Standards Profile IAW Enclosure L

ENCLOSURE J

JOIT C4I PROGRAM ASSESSMENT TOOL - EMPOWERED (JCPAT-E)

1. General. JCPAT-E houses a suite of IT and NSS Interoperability and Supportability based tools that support the official review, assessment, analysis, capabilities certification and certification testing, validation, and document storage/repository requirements for the OASD (NII), Joint Staff J-6 and DISA. It is also the management platform for subordinate tool access, all IT and NSS JCPAT-E Registration Numbers, electronic data storage of finalized J-6 Interoperability and Supportability assessment comments, formal J-6 Interoperability or Supportability Certification memorandums, final JROC/Component Milestone Decision Authority (MDA) validated versions of IT and NSS JCIDS documents (ICD, CDD, CPD and CRD) and ISP, TEMPs and other related interoperability, supportability and applicable joint test information and documentation. There are two subordinate JCPAT-E tools: the Information Support Plan (ISP) Tool (managed by OASD(NII)) and the J-6 Interoperability and Supportability Tool. The ISP tool, managed by OASD(NII), supports the formal staffing, review, comment collection/collaboration and supportability certification of Information Support Plans (ISPs). The J-6 Interoperability and Supportability Tool supports the development of the IT Standards Profile, Interoperability and Interconnectivity Capability (IIC) Profiles for Component Program Managers (PM) use, and pre-JITC testing analysis by the J-6.

2. All JCIDS documents will be staffed by J-8 using the J-8 Knowledge Management/Decision Support (KM/DS) Tool IAW references a and b. OASD(NII), J-6 and DISA interoperability comment collection/collaboration and electronic storage of JCIDS documents will continue to be supported by JCPAT-E.

3. This enclosure provides an overview of JCPAT-E and guidance on use of the JCPAT-E ISP tool for staffing and J-6 Supportability assessment and certification of ISPs. Subsequent enclosures (K and L) provide guidance on unique functions of the J-6 Interoperability and Supportability Tool.

4. JCPAT-E Access

a. JCPAT-E can be accessed via the SIPRNET at https://jcpat.ncr.disa.smil.mil.

b. A user ID and password are required to use the tool. Potential tool users who require accounts may go to the tool home page on the SIPRNET and follow the instructions for requesting a JCPAT-E user account. The instruction explains to a potential user how to submit an online JCPAT-E Access Request Form and send a completed DISA Form 41, System Authorization Access Request (SAAR) to DISA. Once DISA receives the two forms, a JCPAT-E Functional Analyst will establish the user account and notify the new user by SIPRNET E-mail. To contact a JCPAT-E Functional Analyst (FA) refer to the home page of the above Web site.

5. JCPAT-E Functionality. JCPAT-E supports the J-6 Interoperability and Supportability Tool and the OASD(NII) ISP tool with five key management and functional areas that precedes the J-6 interoperability and supportability certifications: 1) User Account Management (UAM) to control tool access, 2) System registration within JCPAT-E, 3) PM development of IT Standards Profiles and IIC Profiles for CDD and CPD documents, 4) Collection/collaboration and storage of interoperability and supportability assessment comments, and 5) Collection and storage of JROC/MDA validated and approved JCIDS and ISP documents in the JCPAT-E Lifecycle Management Repository and Archive via electronic data exchange. These five key areas also precede J-6 interoperability certification in the assessment of JCIDS documents.

6. JCPAT-E Group Responsibilities. JCPAT-E functional analysts place tool users in the following user groups when they establish a user account.

a. ISP Tool Executive Agent (EA). As the EA for this tool, OASD(NII) uses JCPAT-E to automate the process needed to determine OSD Special Interest ISPs, formally task J-6 to staff the review of ACAT I-III and Special Interest ISP documents to combatant commands/Services/ agencies (C/S/A) and OSD staff, and to receive the J-6 Supportability Certification Memorandums that are forwarded to PMs. The results of this process are electronically stored in JCPAT-E Lifecycle Management Repository and Archive, all OASD (NII), J-6 and DISA supportability review/assessment comments and the assessment comments from the J-6's Supportability Assessment Community (See Table J-1 below), and other supportability related documentation. Once the sponsor submits an ACAT ISP in the JCPAT-E ISP tool, within 24 hours the J-6 will staff to C/S/A and OSD for formal Stage I or II assessment with a formal Joint Staff transmittal document (See Figure J-1). OSD Special Interest ISPs will include a transmittal memorandum from OASD(NII).

b. J-6 Interoperability and Supportability Tool Executive Agent (EA). As the EA for this tool, J-6 manages the document repository, IT Standards and Interoperability and Interconnectivity Capability (IIC) Profile development, and pre-JITC testing analysis.

c. ISP Document Submitter Group. Utilizes the ISP tool to submit its documents for formal OASD (NII) review and J-6 supportability assessment and certification. SIPRNET access to JCPAT-E and subordinate tools can be accessed at https://jcpat.ncr.disa.smil.mil.

d. ISP Document Assessor Group. Tool users (See Table J-1 below) who serve as their organization's (C/S/A) primary and alternate POCs are responsible for accessing the J-6 Interoperability and Supportability Tool and performing a required supportability assessment. An automated E-mail will direct the assessor to the ISP Assessment Tool. The document assessor POC is responsible for the following:

(1) Regularly accesses the JCPAT-E ISP tool to account for and respond to all J-6 supportability assessment taskings.

(2) Manages the internal document review for the organization. May assist document reviewers in obtaining a "Read Only" account for an individual document review.

(3) Assists a document reviewer to obtain a username and password for a "Read Only" account for the JCPAT-E ISP tool.

(4) Uses the Comments Review Matrix (CRM) to submit the organization's comments to the JCPAT-E ISP tool.

e. Table J-1 below details the Supportability Assessment Community.

ORGANIZATION	LOCATION	ASSESSMENT TOOL ROLE
OASD (NII)	Crystal Mall III, VA	Support Plan Tool Executive Agent
OASD	Crystal City, VA	Document Assessor
USD(I)	Crystal City, VA	Document Assessor
DOT&E	Crystal City, VA	Document Assessor
AFCA	Scott, AFB	Document Assessor
AT&L	Pentagon, VA	Document Assessor
DCAA	Pentagon, VA	Document Assessor
DeCA	Ft. Lee, VA	Document Assessor
DFAS	Crystal City, VA	Document Assessor
J-6	Pentagon, VA	Document Assessor

DIA/J-2	Pentagon, VA	Document Assessor
DSCA	Pentagon, VA	Document Assessor
DSS	Pentagon, VA	Document Assessor
HQDA	Pentagon, VA	Document Assessor
HQMC	Washington, DC	Document Assessor
DISRMDO	Pentagon, VA	Document Assessor
MDA	Pentagon, VA	Document Assessor
NIMA	Reston, VA	Document Assessor
NRO	Pentagon, VA	Document Assessor
OSD	Pentagon, VA	Document Assessor
OUSD	Pentagon, VA	Document Assessor
USN	Pentagon, VA	Document Assessor
USJFCOM		Document Assessor
USCENTCOM		Document Assessor
USSOUTHCOM		Document Assessor
USSOCOM		Document Assessor
USPACOM		Document Assessor
USEUCOM		Document Assessor
USNORTHCOM		Document Assessor
USTRANSCOM		Document Assessor
USSTRATCOM		Document Assessor

Table J-1. Tool Groups for ISP Assessments

7. Detailed Supportability Certification Procedures

a. System Registration within JCPAT-E. The JCPAT-E IT and NSS Registration Number is an important feature that establishes a system/program link to all related information in the Lifecycle Management Repository and Archive, i.e., profiles documents, certification memorandums, etc. within the JCPAT-E database. System registration in JCPAT-E is required for all systems/capabilities. To register a system, go to SIPRNET URL: http://jcpat.ncr.disa.smil.mil. and click on "Register System" on the lower left hand side of the screen. Then follow the on-line instructions to complete the system registration.

b. Procedures for developing Interoperability and Interconnectivity Capability (IIC) Profiles and IT Standards Profiles. Go to Enclosure K for information on developing IIC Profiles and to Enclosure L for IT Standards Profiles.

c. Supportability Certification of ISP. The process is divided into three stages. Each stage is described step-by-step in the following paragraphs.

(1) Stage I – Draft Assessment. The assessment process is depicted in Figure J-1. Thirty-five (35) calendar days are allocated for a Stage I assessment after a document is submitted through the JCPAT-E

ISP tool. The JCPAT-E Lifecycle Management Repository and Archive is available for C/S/A use to develop documents and search for validated/approved JCIDS documents assessed and certified for interoperability by J-6, and reviewed ISP documents assessed and certified for supportability by J-6. The start of Stage I is the electronic submission by the originating organization (C/S/A) of an ISP document to the JCPAT-E ISP tool. Formal assessments and certification of ISP will occur on the JCPAT-E ISP tool. The tool is used for the comment collaboration/collection, consolidation and for the preparation and storage of the J-6 supportability certification memorandum. The end of Stage I is the submission of the supportability review memorandum to the JCPAT-E ISP tool where it will be subsequently returned to the component sponsor for adjudication of comments and resubmission of the updated ISP and adjudicated comments resolution matrix to the JCPAT-E ISP tool for the Stage II review.

(2) Stage II -- Final Assessment and Certification. The objective of this step is to perform a final assessment of an ISP. The Stage II process is similar to the Stage I process. Twenty-one (21) calendar days are allocated for a Stage II assessment after a document submission. The Stage II assessment and certification process is described in the following steps.

(a) Step 1. Originating C/S/A submits the ISP and its adjudicated Supportability Comments Matrix from the Stage I review electronically via the OASD (NII) tool. Critical Stage I comments are resolved off-line must be incorporated in the Stage II submitted document.

(b) Step 2. For ISPs designated OSD Special Interest, OASD(NII) will create a tasking memorandum and forward to J-6 for formal staffing. The J-6 creates tasking memorandum and suspense date for formal staffing of all ACAT ISPs to documents assessors.

(c) Step 3. The J-6 tool notifies all the Supportability Assessment POCs via automated email that a new ISP document is available for assessment. Assessors review and submit comments back to the JCPAT-E ISP tool. Assessors will only submit critical comments that pertain to the interoperability or supportability certification of the document.

(d) Step 4. J-6 consolidates comments via JCPAT-E ISP tool. Unresolved Stage II critical comments will be forwarded by J-6 to the MCEB or MIB for resolution.

(e) Step 5. J-6 sends Supportability Certification Memorandum to the JCPAT-E ISP tool where it will be subsequently forwarded to OASD(NII) and Component Sponsor (OSD Special Interest ISPs) or the Component Sponsor only (non-OSD Special Interest ISPs).

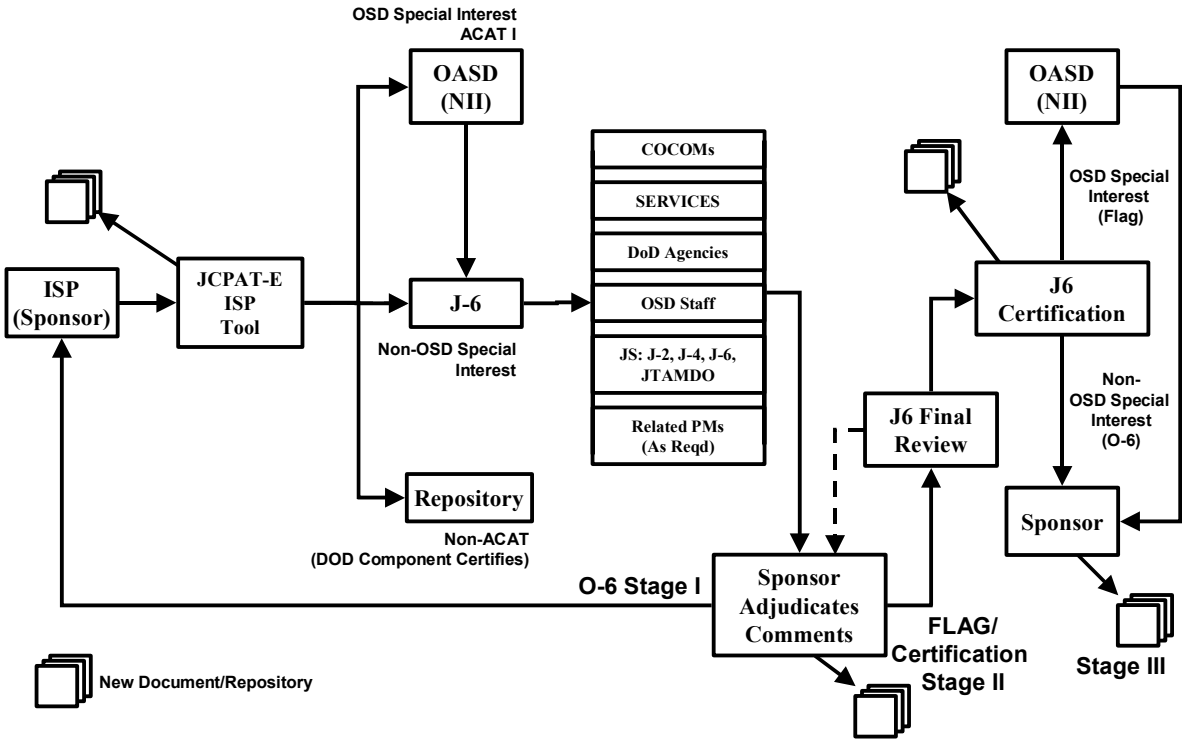

Figure J-1. Supportability Certification Process

(3) Stage III -- Posting of Final Document. Component Sponsors must adjudicate all supportability comments from the Stage II/J-6 Certification review and submit the updated ISP, with its Supportability Comment Matrix to the JCPAT-E ISP tool for J-6 review. The J-6 will use this document to complete and finalize the J-6 Supportability Certification memorandum and submit it to the JCPAT-E ISP Tool for return to the sponsor. As a result of the comments adjudication above, a Stage III action is completed with the posting of the ACAT I, II, III or Special Interest MDA validated/approved ISP to the JCPAT-E Lifecycle Management Repository and Archive. The Stage III goal is 15 calendar days after OASD (NII) reviews and (or) closes out or approves an ISP. Approved documents are filed in the JCPAT-E ISP tool and the JCPAT-E Lifecycle Management Repository and Archive with the J-6 certification letter and other important J-6 and OASD (NII) directed interoperability

and supportability-based information, i.e., IT Standards Profiles, IIC Profiles, applicable joint test information and documentation, i.e., NR-KPPs, etc.

(4) Non-ACAT Program ISPs. Non-ACAT program ISPs will be posted to the JCPAT-E ISP tool by the document sponsor and maintained in the JCPAT-E repository. Non-ACAT ISPs will not be staffed by OASD(NII) or J-6 to C/S/A – the DOD component will ensure sufficiency of the NR-KPP and supportability requirements are met IAW this instruction and other applicable references.

(5) Fielded System ISPs

(a) ISPs for fielded programs which are managed as an acquisition program per DOD 5000 series guidance will be staffed and certified for supportability by OASD(NII) and J-6 IAW the procedures for ACAT ISPs as described above.

(b) All other fielded program ISPs (i.e., for 3 year JITC testing and recertification) will be posted to the OASD(NII) ISP tool by the document sponsor and maintained in the JCPAT-E repository. Fielded ISPs will not be staffed by OASD(NII) or J-6 to C/S/A – the DOD component will ensure sufficiency of the NR-KPP and supportability requirements are met IAW this instruction and other applicable references.

(INTENTIONALLY BLANK)

ENCLOSURE K

INTERCONNECTIVITY AND INTEROPERABILITY CAPABILITY (IIC) PROFILE

1. General. The J-6 Interoperability and Supportability Tool supported by JCPAT-E enables Component Program Managers (PM) to develop the Interconnectivity and Interoperability Capability (IIC) Profile online for joint pre-JITC testing analysis by the J-6 and PMs. The IIC Profile is required as a supporting JCIDS predecessor document for CDDs and CPDs. The JCIDS predecessor requirement mandates the use of the JCPAT-E J-6 Interoperability and Supportability Tool, the JCPAT-E registration number for IT and NSS, and development of IIC Profile by Component PMs. The J-6 Interoperability and Supportability Tool is the management platform and Web-based site for formal IT and NSS interoperability assessment, comment collaboration/collection and J-6 certification determination, generation of JCPAT Registration Numbers, and storage of all DRAFT and final IT Standards Profiles.

2. J-6 Interoperability and Supportability Tool and IIC Profile Development Access

a. The J-6 Interoperability and Supportability Tool may be accessed via the SIPRNET at http://jcpat.ncr.disa.smil.mil.

b. A user ID and password are required to use the tool. Potential tool users who require accounts may go to the tool home page on the SIPRNET and follow the instructions for requesting a JCPAT user account. The instruction explains to a potential user how to submit an on-line JCPAT-E Access Request Form and send a completed DISA Form 41, System Authorization Access Request (SAAR) to DISA. Once DISA receives the two forms, a JCPAT-E Functional Analyst will establish the user account and notify the new user by SIPRNET E-mail. To contact a DISA Functional Analyst for assistance, refer to the JCPAT-E homepage at the above Web site.

3. Background. Supported by the J-6 Interoperability and Supportability Tool, the IIC Profile offers the PM, J-6 and warfighter a Web-based analysis of a system's interoperability at the earliest stages of development. The IIC Profile provides J-6 with the ability to easily consider a system's interconnectivity requirements and known connectivity range in a non-discriminatory manner, while demonstrating a comparative analysis of interoperability between multiple selected

systems prior to the Interoperability Certification IAW JCIDS process, references a and b. The system information PMs/developers provide for the development of the IIC will provide timely knowledge of systems interoperability, capabilities and deficiencies at the front end of the development cycle, insuring interoperability is incorporated from the initiation of the program. Once the IIC Profile database is populated, the J6 Interoperability and Supportability Tool repository can be used to analyze systems against the Joint Integrated Architecture. For specific IIC Profile information, go to URL: http://lisi.ncr.disa.smil.mil.

4. Requirements. An IIC Profile will be developed for all CDDs, CPDs and ISPs. The profile shall be developed via the J-6 Interoperability and Supportability Tool (currently InspecQtor) and be maintained electronically and available for J-6 interoperability assessment and certification determination. The development and availability of IIC will correlate with related CDDs, CPDs submissions during the JCIDS process. Updated versions of IICs can be made periodically via the J-6 Interoperability and Supportability Tool and as new information is available.

5. Applicability. CDDs, CPDs and ISPs will have an IIC Profile associated with them. The IIC Profile shall be a part of the NR-KPP and will be used as an aid in making a final determination by the J6 for Interoperability Certification. The profile for CDDs, CPDs and ISPs consists of two essential elements: Interconnectivity Profile (for CDDs); and Interoperability Capability Profile (for CPDs and ISPs).

a. Interconnectivity Profile. For all CDDs, system interface requirements are captured through system selection and report generation in InspeQtor. This report is utilized for interface requirement comparison with other related CDDs. For profile completion instruction, go to the IIC/Interconnectivity Profile link at http://lisi.ncr.disa.smil.mil.

b. Interoperability Capabilities Profile. For all CPDs and ISPs, the Interoperability Capabilities Profile is created through the Levels of Information Systems Interoperability (LISI) Survey questionnaire completion and report generation in InspeQtor. This report is utilized for interoperability capability comparison with other related CPDs or ISPs. For profile completion instruction, go to the IIC/Interoperability Capability Profile link at http://lisi.ncr.disa.smil.mil.

ENCLOSURE L

IT STANDARDS PROFILE

1. General. J-6 Interoperability and Supportability Tool supported by JCPAT-E enables Component Program Managers (PM) to develop IT Standards Profiles IAW the DOD IT Standards Registry (DISR online). The IT Standards Profile is required as a supporting JCIDS predecessor document for CDDs and CPDs . The JCIDS predecessor requirement mandates the use of the J6 Interoperability and Supportability Tool access, use of the JCPAT-E registration number for IT and NSS, and development of IT Standards Profile by Component PMs. The J6 Interoperability and Supportability Tool is the management platform and Web-based site for formal IT and NSS interoperability assessment, comment collaboration/collection and J6 certification determination, generation of JCPAT Registration Numbers, and storage of all DRAFT and final IT Standard Profiles.

2. J-6 Interoperability and Supportability Tool and DISR online Access.

a. The J-6 Interoperability and Supportability Tool may be accessed via the SIPRNET at http://jcpat.ncr.disa.smil.mil.

b. A user ID and password are required to use the tool. Potential tool users who require accounts may go to the tool home page on the SIPRNET and follow the instructions for requesting a JCPAT user account. The instruction explains to a potential user how to submit an on-line JCPAT-E Access Request Form and send a completed DISA Form 41, System Authorization Access Request (SAAR) to DISA. Once DISA receives the two forms, a JCPAT-E Functional Analyst will establish the user account and notify the new user by SIPRNET E-mail. To contact a DISA Functional Analyst for assistance, refer to the JCPAT-E homepage at the above Web site.

3. Background. Supported by the J-6 Interoperability and Supportability Tool, DISR online enables system developers to identify applicable DISR standards and provides users with an easy method to identify the applicable DOD standards needed and to build an IT system Standards Profile through analysis of the IT and NSS Capability/system requirements. For specific DISR online information, go to URL: http://disronline.disa.smil.mil.

4. Requirements. All CDDs, CPDs, and ISPs will have a standards profile associated with them. This standards profile will be developed via

the DISRonline. The standards profile generated by the DISRonline shall be submitted with its related CDDs, CPDs to the KM/DS during the JCIDS process, and the ISP IAW enclosure J. Updated versions of profiles can be periodically made by the PM. However, only component-approved versions should be submitted with the CDD (DRAFT version) and CPD and ISP (FINAL for record version) versions for subsequent J6 supportability assessment and certification.

5. Standards Profile Development

a. Preparation for IT Standards IAW the DISR begins with the development of a DRAFT Standards Profile for review with the formulation of CDDs and subsequent J-6 interoperability assessment. DISR online shall be utilized to develop all DRAFT Standards Profiles. Once a DRAFT profile is developed, it will be submitted with an assigned JCPAT-E registration number for J-6 interoperability assessment IAW the JCIDS process.

(1) DRAFT Standards Profile development. The PM with appropriate system and IT Standards subject matter experts (SME), with DISR online access and profile building privileges begins the development of a DRAFT Standards Profile.

(2) Producing the DRAFT Standards Profile. A DRAFT Standards Profile is required as a predecessor document to accompany all CDDs being submitted via JCIDS KM/DS. Profiles can be built using one or more of the five profile-building methods. Once the DRAFT profile has been developed, it should be saved for PM level recall and subsequent submission with the CDD IAW enclosure J and the JCIDS process. The DRAFT Standards Profile can be submitted and saved in DISR online.

b. IT Standards developed IAW DISR is initially confirmed for a system when a FINAL Standards Profile is developed for a CPD or with the ISP and its subsequent assessment for J-6 interoperability or supportability. DISR online shall be utilized to develop all FINAL Standards Profiles. Once a FINAL Profile is developed, it will be submitted with an assigned JCPAT-E registration number for J-6 interoperability assessment IAW the JCIDS process.

(1) The PM with appropriate system and IT Standards subject matter experts (SME), with DISR online access and profile building privileges and using previously developed CDD DRAFT Standards Profile, begins to develop a CPD FINAL Standards Profile and (or) ISP FINAL Standards Profile.

(2) Producing the Final Standards Profile and (or) ISP FINAL Standards Profile. A FINAL Standards Profile is required as a predecessor document to accompany all CPDs prior to submission in the JCIDS KM/DS tool. FINAL profiles shall be developed using previously developed DRAFT Standards Profiles and one or more of DISR online's five profile-building methods. Once a FINAL Standards Profile has been developed for a CPD or ISP, it should be saved for PM level recall and subsequent submission with the CPD IAW Enclosure J. The FINAL Standards Profile can be submitted and saved in DISR online.

(INTENTIONALLY BLANK)

ENCLOSURE M

JOINT INTEROPERABILITY TESTING AND TEST CERTIFICATION PROCESS

1. General. All Information Technology (IT) systems, including National Security Systems (NSS), with external interfaces (i.e., top-level information exchange requirements or equivalent interoperability requirements) must be evaluated and certified by the DISA Joint Interoperability Test Command (JITC). All systems – Acquisition Category (ACAT), non-ACAT, and fielded systems – must be evaluated and certified prior to (initial or updated) fielding, and periodically during their entire life – as a minimum, every 3 years. Interoperability is evaluated against Joint Staff J-6 certified NR-KPPs and other approved interoperability requirements. The system PEOs/PMs are responsible for defining and developing the NR-KPPs for each service system. Testing associated with Joint interoperability evaluations may be performed in conjunction with other testing (e.g., Developmental Test & Evaluation (DT&E), Operational T&E (OT&E)) to conserve resources. Information interoperability is a continuous process that must be managed and resourced throughout the system lifecycle. NSA/CSS is the certifier for approved security for protecting classified or national security information (see NSD42).

2. Applicability – Systems Requiring Certification. The intent is that all systems affecting joint information exchange be certified for end-to-end interoperability before being placed into operation [see DOD 4630 series]. This includes, but is not limited to:

a. All systems/programs with a Joint Potential Designation that is not "Independent" (i.e., Joint Impact, Joint Integration, and Joint Interest).

b. All other systems/programs with external interfaces (i.e., top-level information exchange requirements or equivalent interoperability requirements).

c. Joint network infrastructure components (e.g., voice switches for Defense Switched Network (DSN)).

d. Systems regardless of acquisition category or fielded status.

e. Each increment of an evolutionary development, including each spiral of a spiral development.

f. Systems with changes (e.g., DOTMLPF, DOTLPF, hardware or software modifications, including firmware) affecting interoperability, similar changes to interfacing systems, or systems with revoked interoperability certifications or J-6 interoperability system validation, or systems with expired certifications.

3. Joint Interoperability Test Certification. Interoperability Test Certification involves an evaluation of information interoperability with respect to interoperability requirements and capabilities.

a. For systems/programs subject to the JCIDS process, the evaluation will determine the operational information interoperability status of the NR-KPP requirements (including interfaces, top-level exchange requirements and other system interoperability requirements). Systems without JCIDS documents will be evaluated based on equivalent interoperability requirements.

b. Joint Interoperability Test Certification is the part of the overall interoperability certification process that characterizes operational interoperability capabilities and assesses the operational impact of any discrepancies. Related processes are the JOINT STAFF requirements and supportability certifications and the J-6 Joint System Interoperability Validation. J-6 certified requirements and capabilities feed the Joint interoperability test evaluation process, and, in turn, Joint System Interoperability Test Certifications provide input to the J-6 Joint System Validation process and the Milestone Decision Authority (MDA) (or equivalent) fielding decision.

c. JITC issues "full" system certifications when all critical interoperability requirements are met (i.e., all critical interfaces and top-level exchange requirements, or equivalent, are met) and there are no discrepancies with critical operational impact. When appropriate, JITC issues "Specified Interfaces" certifications to provide the system interoperability status when only a subset of critical interfaces have been adequately demonstrated.

d. JITC updates Joint Interoperability Test Certifications throughout a system's lifecycle to reflect changes in the system, status, and environment.

4. Joint Interoperability Test Certification Process. The Joint Interoperability Test Certification process comprises four basic steps. Interoperability testing and evaluation is an iterative process – some or all of the steps may need to be repeated as conditions change. The four basic steps are:

a. Identifying requirements/capabilities.

b. Developing certification approach (planning).

c. Testing & Evaluating.

d. Certifying and other status reporting.

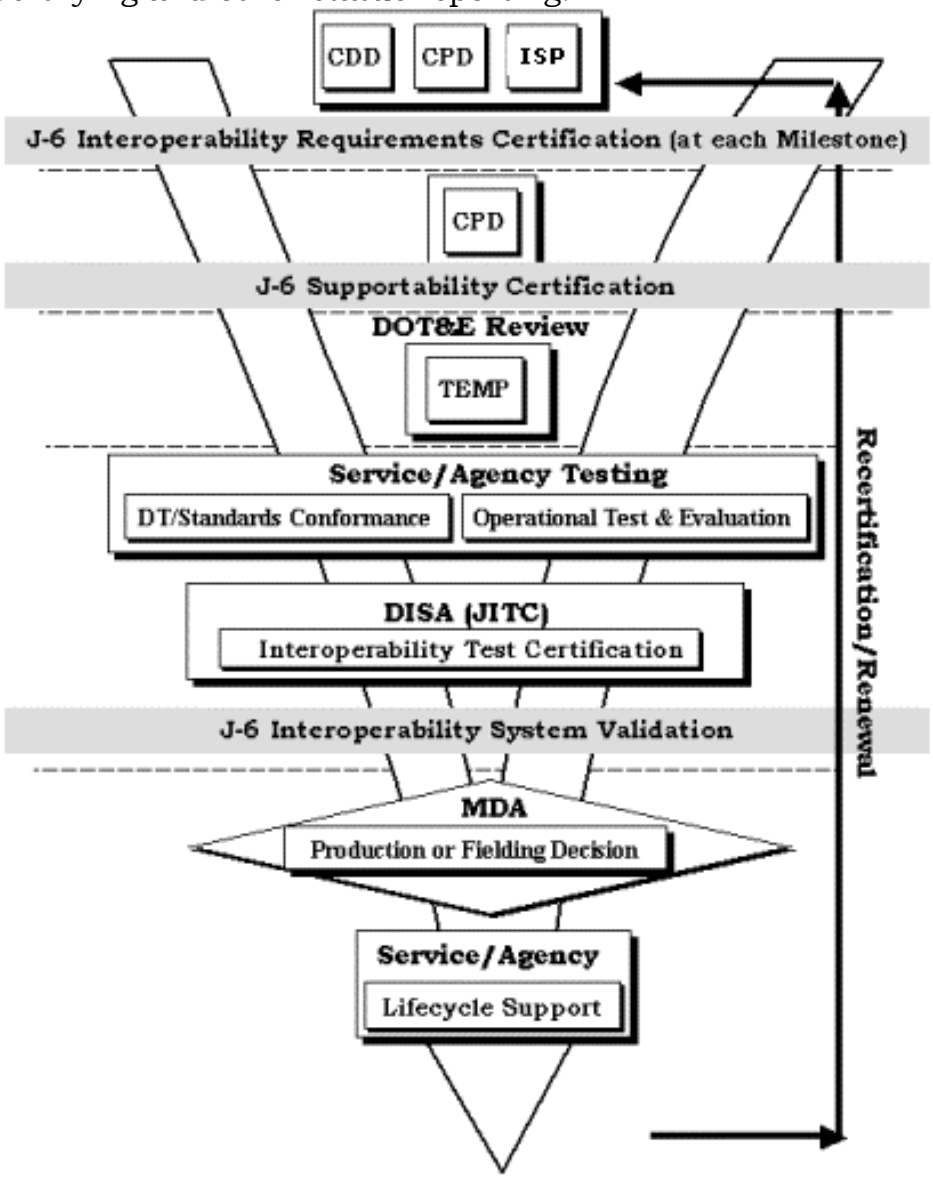

Figure M-1. Interoperability Test Certification

e. Joint Interoperability Test Process Basic Steps:

(1) Identify Requirements/Capabilities. Establishing requirements/ capabilities is a critical step, and system proponents must resolve any requirements/capabilities issues with the Joint Staff J-6. If a J-6 Interoperability System Validation is needed (e.g., for JCIDS systems), requirements/ capabilities must be Joint Staff-certified.

(2) The JITC provides input to the JOINT STAFF requirements/capabilities certification process and uses the results as the foundation for the remaining three steps of the Joint Interoperability Test Certification process. Thus, system proponents must coordinate with the JITC to ensure requirements/ capabilities are defined in measurable and testable form.

(3) Planning. The proponent and JITC will work closely to establish a strategy for evaluating interoperability requirements in the most efficient and effective manner, in an operationally realistic environment. This evaluation strategy identifies data necessary to support interoperability certification as well as the test events/environments planned to produce that data. Proponents will coordinate with JITC to integrate interoperability into the system's T&E documents (e.g., TEMP, test plans). Additionally, complex systems that depend on multiple evaluation events will require JITC to develop an Interoperability Certification Evaluation Plan (ICEP).

(4) Testing and Evaluating. Interoperability evaluation often spans DT and OT and relies on multiple test events conducted by various organizations.

(a) When JITC is not the responsible testing organization, the system proponent will coordinate interoperability test plans, analysis, and reports with JITC to ensure sufficient information is available to support a certification determination. System proponents must coordinate testing changes (e.g., schedule, locations, scope, methodology, etc.) with JITC, since such changes may impact JITC's ability to certify the system.

(b) When JITC is the responsible test organization, JITC will develop the necessary plans and reports and coordinate them with the system proponent. Regardless of the responsible test organization, tests must employ production representative systems in as realistic an operational environment as practicable.

(5) Certification and Status Reporting. JITC uses data from the various types of testing to produce interoperability reports and certifications, as appropriate. Interoperability evaluation will be an independent analysis of the data and determination of the operational interoperability status by JITC. To support the NR-KPP assessment, Joint System Interoperability Test Certifications report on the interoperability status of individual interfaces, the status of top-level exchange requirements, and any other system interoperability performance parameters. JITC distributes Joint System Interoperability Test Certifications to the Military Communications-Electronics Board (MCEB)/Interoperability Test Panel (ITP) members, JOINT STAFF J-6, the program manager, and other interested, authorized parties. JITC interoperability products include the following, though not all products may apply to all systems:

(a) Standards Conformance Certification. Issued after technical testing against published standards to describe the degree of conformance to that standard (e.g., conformance to MIL-STD-188-181 (DAMA SATCOM). A standards conformance certification is not sufficient to allow fielding. Additional testing may be required to determine compliance with standards profiles.

(b) Joint Interoperability Assessment. Issued following interoperability testing (OAs, JITC compatibility and interoperability assessments) to provide feedback concerning interoperability strengths and weaknesses when a certification is not appropriate. An interoperability assessment is not sufficient to allow fielding.

(c) OT Readiness Review (OTRR) Interoperability Statement. JITC input, as appropriate, to the OTRR assessing whether a system is ready for OT from an interoperability perspective.

(d) Joint Interoperability Test Certifications: All JITC interoperability test certifications expire upon changes that may affect interoperability. Additionally, all certifications expire 3 years from date of issue.

1. Special Interoperability Test Certification. Issued for systems or system components (e.g., network infrastructure components) that require operational interoperability certification but are not subject to the JCIDS process, and do not need requirements certified by the JOINT STAFF (e.g., commercial switches being procured to operate in the DSN). Proponents are responsible for adequately defining the interoperability requirements. JITC will work with the JOINT STAFF to

verify that the item is not subject to JOINT STAFF J-6 requirements certification.

2. Joint System Interoperability Test Certification -- Specified Interfaces. Issued when a system has adequately demonstrated operational interoperability for a subset of critical interfaces. A specified interfaces certification may not be sufficient to allow fielding. If military necessity warrants fielding of the system for the demonstrated capabilities, the system proponent should contact the JOINT STAFF J-6 to request a formal modification of the NR-KPP or the MCEB/ITP for an Interim Certificate to Operate (ICTO).

3. Joint System Interoperability Test Certification. Issued when a system has adequately demonstrated operational interoperability for all critical threshold requirements pertaining to a specific release. This full system certification attests that the system's interoperability is sufficient to support a fielding decision. Evaluation should continue until the status of all objective requirements can be determined and reported.

5. Other Considerations. The following must also be considered during the interoperability testing process.

a. Funding for interoperability certification, including planning, testing, analysis, and reporting is the responsibility of the system proponent.

b. JITC Joint Interoperability Test Certification is focused on information exchanges and operational use over external system interfaces. There may also be other certifications, validations, or accreditations required prior to fielding a system (e.g., DODI 5200.40 (DITSCAP), Information Assurance (IA) and security, electromagnetic spectrum, and authorization to connect to specific networks).

6. Related Information

a. The JITC public Web site provides information on available information and access requirements, and points of contact (POCs). Refer to: http://jitc.fhu.disa.mil/.

b. System Tracking Program (STP). JITC uses the STP to track interoperability information for programs and systems. The STP includes information on requirements documentation, ICTOs, and certification status. Authorized users (.mil/.gov) may refer to: https://stp.fhu.disa.mil for instructions on requesting access.

7. Conclusion. The information interoperability certification process must begin during requirements and capabilities development and continue throughout the system lifecycle, including testing and fielding. The intent is to detect interoperability deficiencies sufficiently early to ensure that no system is fielded without demonstrating critical interoperability requirements and/or capabilities. Thorough and continuous coordination among the JOINT STAFF, JITC, and program sponsors is required to ensure that systems provided to the warfighter have met the requisite interoperability requirements to support joint operations.

(INTENTIONALLY BLANK)

ENCLOSURE N

IT AND NSS SPECIFIC POLICIES

1. Purpose. To identify policies on IT and NSS that impact J-6 interoperability and supportability certifications.

2. Policies. JCIDS Requirements and Capabilities documents (ICDs, ORDs, CDDs, and CPDs) must address the following policies on IT and NSS. MNSs that have initiated staffing in the Joint C4I Program Assessment Tool will continue through the normal staffing process; however, J-6 will assess MNSs but will not certify for interoperability requirements certification. J-6 will only concur or non-concur based upon interoperability concerns and implications. IAW references a and b, no new MNS will be accepted for staffing. Existing ORDs will continue to be used until absorbed into the new JCIDS (see reference a).

a. Electromagnetic Environmental Effects (E3)and Spectrum Supportability Policy

(1) All IT and NSS systems must be mutually compatible with other systems in the electromagnetic environment and not be degraded below operational performance requirements due to electromagnetic environmental effects (reference o).

(2) All IT and NSS systems must comply with reference m.

(3) All proposed IT and NSS systems that include spectrum-dependent hardware must document spectrum certification of the hardware (reference m).

(4) Commercial and non-developmental items must also comply with DOD policy on (E3) and Spectrum Supportability (references m and o).

b. Host-nation Approval (HNA). To ensure compatibility as well as interoperability, all IT and NSS with equipment intended for operation in host nations will require HNA coordinated by the MCEB and the appropriate combatant commanders prior to use. Hardware that does not have HNA can be confiscated or denied operation by host nations (reference m).

c. Joint Tactical Radio System (JTRS). All future requirements for radio-based communications will be satisfied by inclusion in the JTRS

CDD unless ASD(NII) grants a waiver. No preplanned product improvements or in-service modifications should be undertaken that duplicate JTRS without prior approval and waiver from ASD (NII) (reference p).

d. Information Assurance. IT and NSS, including commercial and non-developmental items, must comply with applicable DOD IA policies/regulations and Director Central Intelligence Directives (DCIDs). This includes implementation of public key infrastructure (PKI) when required to ensure information security over all voice, video, and data transmission. Interconnection of systems operating at different classification levels will be accomplished by processes approved by the DOD chief information officer (CIO) in conjunction with DIA CIO. IA will be an integral part of all net-readiness efforts thus allowing appropriate security measures to protect mission data and system resources from all known threats (references r, s, t, and u).

e. Hazards of Electromagnetic Radiation to Ordnance (HERO). All proposed IT and NSS systems should be assessed to determine their affect on all electro-explosive devices (ordnance) when the item is employed in IT and NSS systems radio frequency environments.

(1) Ordnance containing electrically initiated devices (EIDs), will be compatible with the operational electromagnetic environment and will not be degraded by E3 (reference o).

(2) Ordnance must be integrated into platforms, systems, and equipment to preclude safety problems and unintentional detonation when exposed to the operational electromagnetic environment (reference o).

ENCLOSURE O

REFERENCES

a. CJCSI 3170.01C, Joint Capabilities Integration and Development System, 24 June 2003

b. CJCSM 3170.01M, Joint Capabilities Integration and Development System, 24 June 2003

c. Interim Defense Acquisition Guidebook (formerly DOD Regulation 5000.2-R, 5 April 2002), 30 October 2002

d. DOD Directive 5000.1, 12 May 2003, "The Defense Acquisition System"

e. DOD Directive 4630.5, 11 January 2002, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

f. DOD Directive 8500.1, 24 October 2002, "Information Assurance"

g. DOD Instruction 4630.8, 2 May 2002, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

h. MCEB Pub 1, 1 March 2002, "Organization, Mission and Functions Manual"

i. DOD Joint Technical Architecture Version 5.1, 12 September 2003

j. C4ISR Architecture Framework, Version 2.0, 18 December 1997

k. CJCSM 3500.04C, 1 July 2002, "Universal Joint Task List"

l. AT&L Knowledge Sharing System (AKSS) located at http://deskbook.dau.mil/jsp/default.jsp.

m. DOD Directive 4650.1, 24 June 1987, "Management and Use of the Radio Frequency Spectrum"

n. DOD Instruction 8800.XX, Draft, DOD Architecture Framework [will replace reference j when published]

o. DOD Directive 3222.3, 20 August 1990, “Department of Defense Electromagnetic Compatibility Program”

p. ASD(C3I) memorandum, 28 August 1998, “Radio Acquisitions”

q. CJCSI 6140.01, 15 November 1998, “NAVSTAR Global Positioning System Selective Availability Anti-Spoofing Module Requirements”

r. AsstSecDef memorandum, 21 May 2002, “Department of Defense (DOD) Public Key Infrastructure (PKI)”

s. ASD (C3I) memorandum, 20 March 1997, “Secret and Below Interoperability (SABI)”

t. DOD Instruction 8500.2, 6 February 2003, “Information Assurance (IA) Implementation,”

u. DOD Instruction 5200.40, 30 December 1997, “DOD Information Technology Security Certification and Accreditation Process (DITSCAP)”

v. DOD Directive 5100.35, 10 March 1998, “Military Communications-Electronics Board (MCEB)”

w. C4ISP Architecture Working Group, 30 March 1998, Levels of Information Systems Interoperability”

x. CJCSI 3180.01, 31 October 2002, “Joint Requirements Oversight Council (JROC) Programmatic Processes for Joint Experimentation and Joint Resource Change Recommendations”

y. DOD Directive 8100.1, 19 September 2002, “ Global Information Grid (GIG) Overarching Policy”

z. DCID 6/1, 1 March 1995, “Security Policy for Sensitive Compartmented Information and Security Policy”

aa. DCID 6/3, 5 June 1999, “Protecting Sensitive Compartmented Information Within Information Systems” (administratively updated 3 May 2002, Directive classified)

bb. (U//FOUO), 26 August 2003, “Top Secret/Sensitive Compartmented Information and Below Interoperability (TSABI) Policy, v4.14”

cc. Global Information Grid (GIG) Architecture Version 2.0, August 2003

dd. National Security Space Acquisition Policy 03-01, 6 October 2003

ee. DODI 5000.2, 12 May 2003, Operation of the Defense Acquisition System

ff. CJCSI 6510.06, 1 May 2001, Communications Security Releases to Foreign Nationals

gg. National Security Directive 42 (NSD-42), 5 July 1990, National Policy for the Security of National Security Telecommunications and Information Systems (CONFIDENTIAL)

hh. NSTISSP Number 11, June 2003, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products

(INTENTIONALLY BLANK)

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
ACTD	Advanced Concept Technology Demonstrations
AIS	Automated Information System
AoA	Analysis of Alternatives
APB	Acquisition Program Baseline
ASD(NII)/DOD CIO	Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer
AT&L	Acquisition Technology and Logistics
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAE	Component Acquisition Executive
C/S/A	Combatant Commands/Services/Agencies
CDD	Capabilities Development Document
CFLC	Community Functional Lead for Cryptology
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CM	Configuration Management
CNO	Chief of Naval Operations
COE	Common Operational Environment
COEA	Cost and Operational Effectiveness Analysis
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf
CPD	Capabilities Production Document
CRC	Control Reporting Center
CRD	Capstone Requirements Document

CSS	Central Security Service
DAA	Designated Approving Authority
DAB	Defense Acquisition Board
DAMA	Demand Assigned Multiple Access
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISA (JITC)	Defense Information System Agency, Joint Interoperability Test Command
DISN	Defense Information Systems Network
DISR	DOD Information Technology Standards Registry
DITSCAP	Defense Information Technology Security Certification and Accreditation Program
DMS	Defense Message System
DOD	Department of Defense
DODD	Department of Defense Directive
DODIIS	DOD Intelligence Information System
DOT&E	Director, Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel and Facility
DT	Developmental Testing
DT&E	Development Testing and Evaluation
DT/OT	Developmental Testing and Operational Testing
E3	Electromagnetic Environmental Effects
ELP	Estimated Launch Point
EMC	Electromagnetic Compatibility
EW	Electronic Warfare
FCB	Functional Control Board
FoS	Family of Systems
FR	Foreign Releasable
FY	Fiscal Year
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GES	GIG Enterprise Services
GIG	Global Information Grid
GIP	Ground Intercept Point
GPS	Global Positioning System

HERO	Hazards of Electromagnetic Radiation to Ordnance
HNA	Host-Nation Approval
IA	Information Assurance
IAP	Information Assurance Panel
ICTO	Interim Certificate To Operate
IAW	In Accordance With
IBS	Integrated Broadcast System
ICD	Initial Capabilities Document
ICEP	Interoperability Certification Evaluation Plan
IER	Information Exchange Requirement
INFOSEC	Information Systems Security
IO	Information Operations
IOC	Initial Operational Capability
ISP	Information Support Plan
ITAB	Information Technology Acquisition Board
ITDC	Interoperability Technology Demonstration Center
ITMRA	Information Technology Management Reform Act of 1996 (Clinger-Cohen Act)
IT	Information Technology
ITP	Interoperability policy and Test Panel
IWL	Interoperability Watch List
JBC	Joint C4ISR Battle Center
JCAPS	Joint C4ISR Architecture Planning and analysis System
JCIDS	Joint Capabilities Integration and Development System
JCPAT	Joint C4I Program Assessment Tool
JITC	Joint Interoperability Test Command
JMETL	Joint Mission Essential Task List
JOA	Joint Operations Area
JROC	Joint Requirements Oversight Council
JROCM	JROC Memorandum
JSC	Joint Spectrum Center
JTA	Joint Technical Architecture
JTE	Joint Test and Evaluation
JTRS	Joint Tactical Radio System
JWCA	Joint Warfighter Capabilities Assessment
JWID	Joint Warrior Interoperability Demonstration

KIP	Key Interface Profile
KM/DS	Knowledge Management/Decision Support
KPP	Key Performance Parameter
LISI	Levels of Information System Interoperability
MAA	Mission Area Analysis
MAIS	Major Automated Information System
MASINT	Measurement and Signature Intelligence
MCEB	Military Communications-Electronics Board
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MIB	Military Intelligence Board
MNS	Mission Need Statement
NATO	North Atlantic Treaty Organization
NCBTS	Noncombatants
NCES	Net Centric Enterprise Services
NCOW	Net Centric Operations and Warfare
NCOW-RM	Net Centric Operations and Warfare Reference Model
NETWARS	Network Warfare Simulation
NGA	National Geospatial-Intelligence Agency
NII	Networks and Information Integration
NIMA	National Imagery and Mapping Agency
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NITF	National Imagery Transmission Format
NR-KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
NSGI	National System for Geospatial Intelligence
NSS	National Security Systems
O	Objective
OHIO	Only Handle Information Once
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT	Operational Testing
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
OV	Operational View

PK	Public Key
PKI	Public Key Infrastructure
PM	Program Manager
PPS	Precise Positioning Service
POC	Point Of Contact
POM	Program Objective Memorandum
PSA	Principal Staff Assistant
PTUC	Participating Test Unit Coordinator
R&D	Research and Development
RAD	Requirements and Acquisition Division
RDT&E	Research, Development, Test, and Evaluation
S	SECRET
SAASM	Selective Availability Anti-Spoofing Module
SABI	SECRET and Below Interoperability
SAMP	System Acquisition Master Plan
SATCOM	Satellite Communications
SCC	Standards Coordinating Committee
SIGINT	Signals Intelligence
SIPRNET	SECRET Internet Protocol Router Network
SoS	System of Systems
STP	System Tracking Program
SWARF	Senior Warfighting Forum
T	Threshold
TAMD	Theater, Air, and Missile Defense
TAOM	Tactical Air Operations Module
TBM	Theater Ballistic Missile
TEMP	Test and Evaluation Master Plan
TOC	Tactical Operations Center
THAAD	Theater High Altitude Area Defense
TRADOC	Training and Doctrine Command (US Army)
TRM	Technical Reference Model
TV	Technical View
UAV	Unmanned Aerial Vehicle
UJTL	Universal Joint Task List
USA	United States Army
USAF	United States Air Force

USCENTCOM	United States Central Command
USEUCOM	United States European Command
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USMS	United States MASINT System
USN	United States Navy
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSID	United States Signals Intelligence Directive
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command

PART II -- DEFINITIONS

Accreditation. The process by which an IT and NSS are evaluated for meeting security requirements to maintain the security of both the information and the information systems. A designated accreditation authority (DAA) is named for each system. Co-DAAs will accredit IT and NSS in certain cases involving interoperability or integration of multiple systems.

Acquisition Category (ACAT). Categories established to facilitate decentralized decision making as well as execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. DOD 5000.2-R, Part 1, provides the specific definition for each acquisition category (ACAT I through III).

ACAT I. A major defense acquisition program (MDAP) subject to Defense Acquisition Board oversight and estimated by the USD(AT&L) to require an eventual total expenditure of more than $355 million in RDT&E funds, or $2.135 billion in procurement funds measured in FY 1996 constant dollars.

ACAT IA. A major automated information system (MAIS) acquisition program that is estimated to require program costs in any single year in excess of $30 million, total program costs in excess of $120 million, or total lifecycle costs in excess of $360 million (FY 1996 constant dollars).

ACAT IAC. A major automated information system acquisition program for which the DOD chief information officer (CIO) has delegated milestone

decision authority (MDA) to the component acquisition executive (CAE) or component CIO. The "C" (in ACAT IAC) refers to component.

ACAT IAM. A major automated information system (MAIS) acquisition program for which the MDA is the DOD CIO.

ACAT IC. A major defense acquisition program subject for which the MDA is the DOD component head, or if delegated, the DOD component acquisition executive (CAE). The "C" refers to component.

ACAT ID. MDAP for which the MDA is USD (AT&L). The "D" refers to the Defense Acquisition Board (DAB), which advises the USD(AT&L) at major decision points.

Administrative comments. Administrative comments to correct what appear to be typographical or grammatical errors.

Architecture. The structure, relationships, principles and guidelines that governs component design and evolution.

Automated Information System (AIS). A combination of computer hardware and computer software, data, and/or telecommunications that performs functions such as collecting, processing, storing, transmitting and displaying information. Excluded are computer resources, both hardware and software, that are: physically part of, or dedicated to, or essential in real time to the mission performance of weapons systems; used for weapon system specialized training, simulation, diagnostic test and maintenance, or calibration; or used for research and development of weapon systems.

Certification. A statement of adequacy provided by a responsible agency for a specific area of concern in support of the validation process. Certification consists of three forms of capability confirmation -- first, one that addresses system interoperability requirements; second, one that addresses supportability; and third, one that addresses total life-cycle oversight of warfighter interoperability requirements. The two J-6 certifications and validation are discussed below.

a. J-6 Developmental and Production Capabilities Interoperability Certification. This certification occurs prior to each acquisition milestone (B, C). The J-6 certifies ORDs, CDDs, CPDs and ISPs regardless of ACAT level, for conformance with joint IT and NSS policy and doctrine and interoperability standards. As part of the review process, J-6 requests assessments from the Services, OSD, DISA and DOD agencies.

b. J-6 Supportability Certification. The J-6 certifies to OASD(NII) that programs, regardless of ACAT, adequately address IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems. As part of the review process, J-6 requests supportability assessments from DISA and DOD agencies. J-6 conducts a supportability certification for CPD, prior to Milestone C for submission to OASD(NII) as part of the CPD review process.

c. J-6 Interoperability System Validation. The J-6 validation is intended to provide total lifecycle oversight of warfighter capabilities interoperability. The J-6 validates the DISA (JITC) interoperability system test certification, which is based upon a joint certified NR-KPP, approved in the CDD, CPD and ISP. The validation will occur after receipt and analysis of the DISA (JITC) interoperability system test certification. The J-6 will issue an interoperability system certification memorandum to the respective Services, agencies, and developmental and operational testing organizations.

C4I Support Plans (C4ISP). A document that provides a window into a specific system development program through which can be seen any shortfalls in the intelligence support, IT and NSS required for each phase of the system's lifecycle.

Capability Gaps. Those synergistic resources (DOTMLPF) that are unavailable but potentially attainable to the operational user for effective task execution.

Capability Production Document (CPD). A document that addresses the production elements specific to a single increment of an acquisition program.

Capstone Requirements Document (CRD). A document that contains capabilities-based requirements that facilitates the development of CDDs and CPDs by providing a common framework and operational concept to guide their development.

Coalition interface. Any interface that passes information between one or more US IT and NSS and one or more coalition partner IT and NSS.

Combined interface. Any interface that passes information between one or more US IT and NSS and one or more allied IT and NSS.

Computer resources. Components physically part of, dedicated to, or essential in real time to mission performance; used for weapon system

specialized training, simulation, diagnostic test and maintenance or calibration; or used for research and development of weapon systems.

Communities of Interest (CoI). Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange (source: DCIO DOD Net-Centric Data Strategy, dated 9 May 2003)

Critical comments. Critical comments will cause non-concurrence in a document if comments are not satisfactorily resolved. During a flag-level review, persons commenting are required to contact and coordinate critical comments with document submitters prior to submission of the comments.

Defense Information Infrastructure (DII). Outdated term: the DII is the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of DOD users across the range of military operations. It encompasses:

a. **Sustaining base**, tactical, IT and NSS.

b. **Physical facilities** used to collect, distribute, store, process, and display voice, data and imagery.

c. **Applications** and data engineering tools, methods and processes to build and maintain the software that allow command and control (C2), intelligence, surveillance, reconnaissance, and mission support users to access and manipulate, organize and digest proliferating quantities of information.

d. **Standards** and protocols that facilitate interconnection and interoperation among networks.

e. **People** and assets, which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities and train others in DII capabilities and use.

f. DOD Information Technology Standards Registry (DISR).

g. **Replacement** for the DOD Joint Technical Architecture (JTA). It will also be accessible via the Internet.

DOD Joint Technical Architecture (DOD JTA). The DOD JTA provides DOD systems with the basis for the needed seamless interoperability. The DOD JTA defines the service areas, interfaces, and standards (DOD JTA elements) applicable to all DOD systems. Its adoption is mandated for the management, development and acquisition of new or improved systems throughout DOD. The DOD JTA consists of the core, four domains, and numerous subdomains. The DOD JTA core contains the minimum set of DOD JTA elements applicable to all DOD systems to support interoperability. Standards and guidelines contained in the DOD JTA are stable, technically mature and publicly available. In addition, the JTA online system provides a Web-based capability for creating DOD JTA standard complaint profiles that can be used to build a TV-1 or TV-2. (http://jtaonlline.disa.mil). ASD(NII) is currently transforming the JTA to the DOD Information Technology Standards Registry (DISR) to better support the business and warfighting domains. It will also be accessible via the Internet.

Electromagnetic compatibility (EMC). The ability of systems, equipment and devices that use the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation response. It involves the application of sound electromagnetic Spectrum Supportability; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic environmental effects (E3). E3 is the impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including compatibility, interference; vulnerability, pulse; protection; hazards of radiation to personnel, ordnance, and volatile materials; and natural phenomena effects, of lightning and p-static.

Family-of-systems. A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. The mix of systems can be tailored to provide desired capabilities dependent on the situation.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information

superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security Systems, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

Information assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Joint Publication 3-13).

Information exchange requirements. Information exchange requirements (IERs) characterize the information exchanges to be performed by the proposed system(s). For CDDs, top-level IERs are defined as those information exchanges that are between systems of combatant command/Service/agency, allied, and coalition partners. For CPDs, top-level IERS are defined as those information exchanges that are external to the system (i.e., with other combatant commands/Services/agencies, allied and coalition systems). IERs identify **who** exchanges **what** information with **whom**, **why** the information is necessary, and **how** the information exchange must occur. Top-level IERs identify warfighter information used in support of a particular mission-related task and exchanged between at least two operational systems supporting a joint or combined mission. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement.

Information Support Plan (ISP). Used by program authorities to document the IT and NSS needs, objectives, interface requirements for all non-ACAT and fielded programs. ISPs should be kept current throughout the acquisition process and formally reviewed at each milestone, decision reviews and whenever the operational concepts, and IT and NSS support requirements change.

Information technology (IT). Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support

services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Initial Capabilities Document (ICD) - Documents the need for a materiel solution to a specific capability gap derived from an initial analysis of alternatives executed by the operational user and, as required, an independent analysis of alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects, and time.

Integrated Architecture. An architecture consisting of multiple views or perspectives (Operational View, Systems View, and Technical Standards View) that facilitates integration and promotes interoperability across family of systems and system of systems and compatibility among related architectures. An architecture description that has integrated Operational, Systems, and Technical Standards Views with common points of reference linking the Operational View and the Systems View and also linking the Systems View and the Technical Standards View. An architecture description is defined to be an *integrated architecture* when products and their constituent architecture data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view.

Intelligence certification. Confirmation by DIA of the availability, suitability, and sufficiency of intelligence to support a system or program. Intelligence certification also provides: (1) an assessment of the impact of a system or program on joint intelligence strategy, policy, architectural planning, and needs of the warfighter and (2) an evaluation of open systems architectures, interoperability, and compatibility for intelligence handling and intelligence-related information systems. This certification will occur as a prerequisite for the system acquisition process and at each acquisition milestones.

Interim Certificate to Operate (ICTO). Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

Interoperability. a. The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively

together, and b. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them or their users. The degree of interoperability should be defined when referring to specific cases. For the purposes of this instruction, the degree of interoperability will be determined by the accomplishment of the proposed IER fields.

Interoperability Watch List (IWL). Established by the USD(AT&L), the ASD(NII)/DOD CIO, the Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Joint Forces Command to provide DOD oversight for those IT and NSS activities for which interoperability is deemed critical to mission effectiveness, but interoperability issues are not being adequately addressed. IT and NSS considered for the IWL may be pre-acquisition systems, acquisition programs (any ACAT), already fielded systems, or combatant commander-unique procurements.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (Joint Publication 3-13).

Joint C4ISR Architecture Planning/Analysis System (JCAPS). DOD-approved static architecture tool for manipulating and conducting analysis of operational and systems architectures.

Joint integrated architecture. An integrated architecture that establishes the basis for rapidly acquiring affordable and evolving joint warfighting capabilities through collaborative planning, analysis, assessment, and decision making.

Joint interface. An IT and NSS interface that passes or is used to pass information between systems and equipment operated by two or more combatant commanders, Services, or agencies.

JROC special interest. Programs identified by the JROC Secretary as being of interest to the JROC for oversight even though they do not meet the ACAT I cost thresholds or have been designated as ACAT ID.

Levels of Information System Interoperability (LISI). A model that is applied to information systems to gain a figure of interoperability between systems. Within the LISI model, systems are evaluated by their use, application, sharing and/or exchange of common procedures (to include technical standards), software applications, infrastructure and data. The resultant value, from 0 to 4, indicates the interoperable maturity levels of Isolated (0), Connected (1), Functional (2), Domain (3) and Enterprise (4).

Key Interface. Interfaces in functional and physical characteristics that exist at a common boundary with co-functioning items, systems, equipment, software and data. They are designated as a Key Interface when one or more of the following criteria are met:

a. The interface spans **organizational boundaries**. Different entities (service, agency, organization) have ownership and authority over the hardware and software capabilities on either side of the boundary,

b. The interface is **mission critical**. Data from joint organizations, multiple services, and/or multiple agencies/organizations must move across the interface to satisfy joint information flow requirements. If systems are not interoperable at that interface, the ability to accomplish the mission is endangered.

c. The interface is difficult or complex to manage.

d. There are **capability, interoperability, or efficiency** issues associated with the interface.

e. The interface **impacts multiple acquisition programs**, usually more than two (e.g. network points of presence, many-to-many or one-to-many connections).

f. The interface is **vulnerable** or important from a security perspective.

Key Interface Profile (KIP). An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, Interface Control Document/Specifications, Engineering Management Plan, Configuration Management Plan, Technical View with SV-TV Bridge, and Procedures for Standards Conformance and Interoperability Testing.

Key performance parameters (KPPs). Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet a system or program's KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a system or program's KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC. KPPs are included in the acquisition program baseline.

Milestone decision authority (MDA). The individual designated in accordance with criteria established by the USD(AT&L), or by the ASD (NII) for acquisition programs, to approve entry of an acquisition program into the next phase.

Milestones. Major decision points that separate the phases of an acquisition program.

Mission need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance existing capabilities) through the use of new technologies. They are expressed in broad operational terms by the DOD components.

Mission needs statement (MNS). A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept Exploration and Definition Phase of the Requirements Generation Process. (Joint Publication 3-13).

National Security Systems (NSS). Telecommunications and information systems operated by the Department of Defense -- the functions, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves the command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons systems; or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).

Net-Centricity. Net-centricity enables user access and use of resources both collaboratively and asynchronously, regardless of time and place. It is the ability of a program or system to integrate with, offer services to, and exploit the services of a net-centric environment.

Net Centric. Exploitation of advancing technology that moves from an applications-centric to a data-centric paradigm - that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.

Net Centric Operations and Warfare (NCOW). Describes how DOD will conduct business operations, warfare, and enterprise management. It is based on the concept of an assured, dynamic, and shared information environment that provides access to trusted information for all users,

based on need, independent of time and place. It is characterized by assured services, infrastructure transparency (to the user), independence of data consumers and producers, and metadata supported by information discovery, protection and mediation. This fundamental shift from platform-centric warfare to net-centric warfare provides for an Information Superiority-enabled concept of operations. The NCOW RM provides a common taxonomy and lexicon of NCOW concepts and terms, and architectural descriptions of NCOW concepts. It represents an important mechanism in DOD transformation efforts, establishing a common framework for net-centricity. It will enable capability developers, program managers, and program oversight groups to move forward on a path toward a transformed, net-centric enterprise. Parameter.

Net Centric Operations and Warfare Reference Model (NCOW RM). Reference Model (NCOW RM). The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic user-interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (CoI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DOD information technology capabilities and the Net Ready Key Performance

Net-Ready. DOD IT/NSS that meets required information needs, information timeliness requirements, has information assurance accreditation, and meets the attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. DOD IT/NSS that is Net-Ready enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants. Net-readiness requires that IT/NSS operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure seamless communications within and across diverse

Media; information is in a common format with a common meaning; there exist common human-computer interfaces for users; and there exists effective means to protect the information. Net-Readiness is critical to achieving the envisioned objective of a cost-effective, seamlessly integrated environment. Achieving and maintaining this vision requires interoperability:

a. Within a Joint Task Force/combatant command area of responsibility (AOR).

b. Across combatant command AOR boundaries.

c. Between strategic and tactical systems.

d. Within and across Services and agencies.

e. From the battlefield to the sustaining base.

f. Among US, Allied, and Coalition forces.

g. Across current and future systems.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements: a. Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), b. Compliance with applicable GIG Key Interface Profiles (KIPs), c. Verification of compliance with DOD information assurance requirements, d. Supporting integrated architecture products required to assess information exchange and use for a given capability.

Net-Ready KPP Assessment. The Net-Ready KPP Assessment determines the impacts, risks, and vulnerabilities of fielding secure, interoperable, supportable, sustainable and usable (SISSU) systems to the warfighter. Parameters assessed include: network security, network impact, compatibility with the infrastructure, infrastructure requirements, spectrum support, security policy compliance, DISR standards compliance, communications and information manpower, training, logistics support, schedule and funding. A system that has been assessed and determined to be supportable from a communications and

information perspective, and any impacts, risks and vulnerabilities that it may present to the enterprise are deemed to be acceptable or manageable is Net Ready.

Network warfare simulation (NETWARS). The standard DOD approved communications simulation tool. Combatant commanders, Services and agencies use NETWARS for all communications modeling purposes.

Non-Acquisition (Non-ACAT) Program. An effort that does not directly result in the purchase of a system or equipment for operational employment (e.g., science and technology programs, concept exploration or advanced development of potential acquisition programs).

Operational requirements document (ORD). A formatted statement-containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with milestone I. Upon publication of CJCSI 3170.01C, new ORDs will be accepted for only 90 days. Existing ORDs will continue to be used until absorbed into the new JCIDS (see reference a).

Originator. A DOD component or operational command that initiates a MNS. The originator may or may not be the sponsor.

Procedural interface. The methods and procedures employed to establish an interconnection within and between systems or equipment and to transfer information within or between systems or equipment.

Requirement. The need of an operational user initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the CDD.

Seamless IT and NSS environment. An electronic environment that allows data to be accessed by the warfighter without regard to physical or electronic boundaries.

Service deployment plans and fielding plans. Plans that describe the evolution from current capabilities to the full operational capability for new or modified IT and NSS. Included are fielding schedules, plans, locations, and associated time-phased interoperability capabilities and requirements with current and planned systems of other DOD components or allies.

Spectrum certification. The process by which development or procurement of communication-electronics systems, including all systems employing satellite techniques, will be reviewed and certified for

system compliance with Spectrum Supportability policy, allocations, regulations, and technical standards to ensure that radio frequency spectrum is available. Additionally, the predicted degree of electromagnetic compatibility between the proposed system and other spectrum-dependent systems; and the possible need for and evaluation of the results of prototype electromagnetic compatibility testing will be determined.

Spectrum Supportability. The determination as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or system during its expected lifecycle is, or will be, available (that is, from system development, through developmental and operational testing, to actual operation in the electromagnetic environment.) The assessment of equipment or system as having "spectrum supportability is based upon, as a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of electromagnetic compatibility (EMC).

Standardization approach. A statement(s), which demonstrates a commitment to use DOD, approved standards. For example, "The system must comply with applicable information technology standards contained in the DOD Information Technology Standards Registry (DISR) current version."

Standards. Standards as referenced in this instruction are information technology (IT) standards and include specifications, profiles, protocols, implementation conventions, Federal Information Processing Standards (FIPs), Military Standards (MIL-STDs), Defense Performance Specifications (MIL-PRFs), NATO Standardization Agreements (STANAGs), Allied Communications Publications (ACPs), Allied Data Publications (ADatP), guidelines, commercial item descriptions, standardized drawings, handbooks, manuals, tools, and other related documents relevant to the application and use of information and communications technology. They are software and hardware standards that are used for intelligence collection, data and information processing, information transfer, and information presentation/ dissemination. IT standards provide technical definitions for information system processes, procedures, practices, operations, services, interfaces, connectivity, interoperability, information formats, information content, interchange, and transmission of transfer. IT standards apply during the development, testing, fielding, enhancement, and lifecycle maintenance of DOD information systems. Recognized standards include those produced as non-governmental national or international standards (e.g., ANSI and ISO), trade association and professional society standards (e.g.,

IEEE), Federal standards (e.g., FIPS), military standards, and multinational treaty organization standardization agreements.

Substantive comment. Substantive comments are provided because sections in the document appear to be or are potentially unnecessary, incorrect, incomplete, misleading, confusing, or inconsistent with other sections.

Supportability. The level that programs, regardless of ACAT, adequately address IT and NSS infrastructure requirements, the availability of bandwidth and spectrum support, funding, personnel, and identify dependencies and interface requirements between systems.

SV-1. High-level system interface description

System. For use in this publication, the term "system" refers to a system or program. A practical definition is that a "system" will follow the complete Joint Capability Integration and Development System (JCIDS) (Requirements Generation System (RGS)) process.

Technical View. An architecture view that describes in engineering terms how to tie systems together. It consists of standards that define and clarify the individual systems technology and integration requirements.

Validation. The review of documentation by an operational authority other than the user to confirm the operational capability. Validation is a precursor to approval.

Validation Authority. The individual within the DOD components charged with overall capability definition and validation. The Vice Chairman of the Joint Chiefs of Staff, in the role as the Chairman of the JROC, is the validation authority for all potential major defense acquisition programs. The validation authority for JCIDS issues is dependent upon the JPD of the program or initiative as specified below:

a. **JROC Interest** - JROC is validation authority.

b. **Joint Impact** - The lead FCB is the validation authority.

c. **Joint Integration** - The sponsor is the validation authority.

d. **Independent** - The sponsor is the validation authority.